

PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE E TRASPARENZA

2023-2025

Ai sensi della Legge 190/2012 “*Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella Pubblica Amministrazione*” e s.m.i., Arezzo Telematica S.p.A. adotta solitamente entro il 31 gennaio di ogni anno, un Piano Triennale di Prevenzione della Corruzione con la funzione di prevedere una serie di misure finalizzate a contrastare il verificarsi di fenomeni di corruzione nelle Amministrazioni Pubbliche sia centrali che locali ed anche negli enti di diritto privato a controllo pubblico quale è Ar.tel. S.p.A. Per individuare le attività maggiormente esposte al rischio di corruzione e prevenire attività illegittime o illecite, la Società adotta procedure, comportamenti interni e sistemi di controllo finalizzati a migliorare l’efficienza e l’efficacia dell’azione amministrativa attraverso:

- l’individuazione delle aree a rischio di corruzione e valutazione delle stesse;
- l’adozione delle misure di prevenzione con lo scopo di ridurre le opportunità, aumentare la capacità di controllo e sfavorire contesti a rischio di corruzione;
- l’individuazione di criteri guida per lo svolgimento delle attività a rischio e per la predisposizione di procedure da osservare;
- la nomina dei soggetti preposti al controllo e alla prevenzione della corruzione;
- l’utilizzo di sistemi di controllo e prevenzione della corruzione

È opportuno segnalare che Legge n. 190/2012, con cui è stata data attuazione nel nostro ordinamento alla Convenzione di Merida, non contiene una definizione distinta di “corruzione”. Dalla *ratio legis* è possibile tuttavia evincere un significato ampio di corruzione a cui si riferiscono gli strumenti e le misure previsti dal Legislatore. Pertanto, l’A.N.A.C., anche in linea con la nozione accolta a livello internazionale, ha ritenuto che, poiché la Legge n. 190/2012 è finalizzata alla realizzazione di una tutela preventiva, debba essere privilegiata un’accezione ampia del concetto di corruzione, volta a ricomprendere, come indicato nel PNA (Piano Nazionale Anticorruzione) 2017, le varie situazioni in cui, nel corso dell’attività amministrativa, si rilevi l’abuso da parte di un soggetto del potere a lui conferito, al fine di ottenere vantaggi privati. Al termine “corruzione” è dunque attribuito un significato più esteso di quello strettamente connesso con le fattispecie di reato disciplinate negli articoli 318, 319 e 319-ter del Codice Penale (ipotesi di corruzione per l’esercizio della funzione, corruzione per atto contrario ai doveri d’ufficio e corruzione in atti giudiziari), tale da comprendere non solo l’intera gamma dei delitti dei pubblici ufficiali contro la Pubblica Amministrazione (disciplinati nel Titolo II, Capo I, del Codice Penale), ma anche le situazioni in cui - a prescindere dalla rilevanza penale – si evinca

un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite ovvero l'inquinamento dell'azione amministrativa *ab externo*, sia che tale azione abbia successo sia nel caso in cui rimanga a livello di tentativo. Con delibera n. 72/2013, CIVIT (oggi ANAC) ha approvato il Piano Nazionale Anticorruzione come predisposto dal Dipartimento della Funzione Pubblica (DFP) e trasmesso dal Ministero della Pubblica Amministrazione e Semplificazione: il predetto PNA, diversamente da quanto previsto nel testo letterale della legge 190/2012, prevede che "I contenuti del presente PNA sono inoltre rivolti alle società partecipate ed a quelle da esse controllate ai sensi dell'art. 2359 c.c. per le parti in cui tali soggetti sono espressamente indicati come destinatari" (paragrafo 1.3 PNA, intitolato "Destinatari.")

CONTESTO ESTERNO

L'analisi del contesto esterno è indispensabile per un'efficace valutazione degli eventuali rischi che potrebbero concretizzarsi nelle attività di Ar.tel. S.p.A.; la naturale conseguenza è l'elaborazione di un PTPCT conforme alla realtà socio-economica in cui opera la Società per una gestione dei rischi mirata ed efficiente.

La pandemia ha avuto un impatto molto forte sulle dinamiche sociali ed economiche nazionali ed internazionali, determinando in Italia (ma non solo in Italia) una sensibile recessione. Il momento di crisi ha rappresentato e costituisce ancora un'opportunità per le organizzazioni criminali di incrementare i propri business illeciti ed estendere la base del consenso sociale. Si registrano, inoltre, forme di imprenditorialità diretta e di infiltrazione nella pubblica amministrazione per la gestione di appalti.

Il costante monitoraggio è stato operato nella consapevolezza che i flussi di denaro, nazionali e comunitari, destinati a sostenere l'economia ed a rilanciare la fase di ricostruzione post emergenza risultano particolarmente appetibili da parte delle organizzazioni mafiose (per le quali è strategico inserirsi nei circuiti legali per riciclare il denaro). In questo scenario, di particolare importanza risulta il lavoro dell'Organismo permanente di monitoraggio e analisi sul rischio di infiltrazioni nell'economia da parte della criminalità organizzata di tipo mafioso. Si tratta di una struttura interforze, composta da rappresentanti della Polizia di Stato, dell'Arma dei Carabinieri, della Guardia di Finanza, del Ministero della Giustizia, della Direzione Investigativa Antimafia, della Direzione Centrale per i Servizi Antidroga e del Servizio Polizia Postale e delle Comunicazioni della Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato.

L'obiettivo è quello di condividere le informazioni di cui dispongono le Forze di polizia per intercettare i sintomi e le tendenze criminali in chiave preventiva e di contrasto investigativo; lo scenario, tuttavia, non può essere limitato ai confini nazionali, dato che la pandemia e la conseguente recessione economica hanno assunto dimensioni globali, come è globale la minaccia rappresentata dalle

infiltrazioni della criminalità organizzata, specie mafiosa, a livello intercontinentale.

Da uno studio effettuato, invece, dalla Regione Toscana in collaborazione con l'Università di Pisa, emergono dati preoccupanti sulle attività corruttive e criminose nel territorio toscano. L'ultimo rapporto disponibile analizza gli studi effettuati nell'anno 2020.

Gli episodi del 2020 rendono sempre più intellegibili i caratteri di una specifica "variante" toscana rispetto ai fenomeni di riproduzione criminale delle mafie nazionali e transnazionali nella regione. In Toscana queste organizzazioni mostrano una forte vocazione imprenditoriale, che trova realizzazione nel tessuto economico locale attraverso investimenti di capitali illeciti sia per fini di mero riciclaggio, sia con l'obiettivo di fare impresa, operando attivamente nel mercato regionale e anche fuori i confini regionali.

Nel corso del 2020, non sono emersi elementi che facciano ipotizzare un radicamento organizzativo tradizionale delle mafie nazionali in Toscana, sebbene alcune criticità ambientali, aggravate dagli effetti economici della crisi sanitaria, possono creare nuove opportunità criminali per attività di riciclaggio e di imprenditorialità mafiosa, prodromiche di una presenza organizzativa più incisiva e penetrante. In base all'analisi dei principali eventi riferibili a fenomeni di criminalità organizzata di origine nazionale osservati in Toscana (circa 42 eventi analizzati nel 2020), la proiezione criminale di organizzazioni di matrice camorristica risulta la più diffusa ed eterogenea per strategie di business criminale sul territorio regionale (38% degli eventi analizzati). Gli eventi riconducibili a gruppi con una matrice 'ndranghetista in Toscana (29%), invece, confermano l'elevata capacità di queste consorterie criminali sia nel promuovere attività illecite su larga scala, come nel caso del traffico internazionale di stupefacenti, sia nel condizionare l'economia legale, attraverso il coinvolgimento di operatori economici toscani in cartelli di imprese finalizzati alla manipolazione del mercato dei contratti pubblici o di settori economici ad elevata regolazione (es. rifiuti). Infine, gli eventi relativi ad organizzazioni di origine siciliana (21%) rivelano il perdurare di relazioni tra gruppi ancora operativi nell'isola e soggetti da tempo trasferitisi sul territorio toscano.

Gli eventi relativi ad associazioni criminali di matrice transnazionale (32 casi analizzati nel 2020) mostrano la sempre maggiore organizzazione e dimensione dei traffici illeciti promossi da gruppi in gran parte di origine albanese (31%), cinese (28%), nigeriana (18%), e dalla composizione mista. Il traffico di stupefacenti rappresenta il principale business criminale (66% dei casi), seguito dal favoreggiamento della migrazione clandestina (25%) e da reati di caporalato e tratta (16%). In molti degli eventi analizzati è stata contestata l'associazione a delinquere semplice o per traffico (65%), mentre permangono le difficoltà di un eventuale qualificazione giuridica della matrice mafiosa delle organizzazioni più strutturate presenti sul territorio.

Rispetto alle attività economiche, le attività di contrasto e prevenzione patrimoniale evidenziano ancora una volta in Toscana un interesse specifico da parte delle organizzazioni criminali rispetto agli

investimenti nel settore privato (immobiliare, alberghiero, ristorazione, costruzioni), in misura anche maggiore rispetto al mercato dei contratti pubblici. La vulnerabilità del settore privato si è aggravata per via dell'incremento di domanda di capitali e di compravendite di attività economiche in difficoltà finanziarie dovute all'emergenza sanitaria, e per un sistema di monitoraggio e di filtro antimafia ancora sottoutilizzato in questo ambito. L'economia sommersa, i settori economici a legalità debole e quelli nei quali sono più diffuse forme di criminalità economica e finanziaria, costituiscono il principale canale di infiltrazione criminale delle mafie nel territorio toscano, con una vulnerabilità financo maggiore ad altri canali più tradizionali, fra tutti quello del mercato dei contratti pubblici. Secondo i dati U.I.F. di Banca d'Italia, nel 2020 tra le prime quindici province italiane per numero pro-capite di segnalazioni sospette tre sono toscane (Prato, Siena e Firenze), con quella di Prato che conferma il primato nazionale. Il numero complessivo di segnalazioni in Toscana è diminuito rispetto al 2019 (-2,5%), in controtendenza rispetto al dato nazionale (+7%). Secondo un indicatore di anomalie nell'uso del contante elaborato dallo stesso U.I.F., 9 province toscane su 10 presentano un rischio medio-alto o superiore, con un dato regionale complessivo tra i più significativi in Italia. Secondo i dati della D.I.A., sono aumentate del 200% il numero di segnalazioni sospette analizzate dalla Direzione Investigativa (in linea con il trend nazionale), per un totale di oltre 20 mila segnalazioni. Un terzo di queste è stato ricondotto a possibili fenomeni di criminalità organizzata, il restante a c.d. reati spia. Rispetto al mercato dei contratti pubblici e delle concessioni/ autorizzazioni, la Toscana è la terza regione del Centro Nord Italia per numero di provvedimenti interdittivi emessi dalle prefetture nel corso del 2020, con una quota pari al 4,5% del totale nazionale, in aumento del 270% rispetto all'anno precedente (34 provvedimenti contro i 9 del 2019). Incidenza maggiore nei settori del commercio, costruzioni e servizi, confermando la vulnerabilità sia dei lavori che dei servizi.

Per quanto riguarda la **Provincia di Arezzo**, il *Sole 24 Ore* ha pubblicato la classifica della criminalità delle città italiane relativa all'anno 2021: Arezzo occupa il 72esimo posto sulle 106 province del Belpaese prese in esame, con un indice in calo dell'8,4% rispetto al 2019. Il confronto è stato fatto con l'ultimo anno prima delle chiusure Covid, le limitazioni, infatti, hanno fatto crollare le statistiche dei delitti per quanto riguarda l'anno 2020. L'indice della criminalità è calcolato in base alle denunce fatte: nell'Aretino, nel corso del 2021, sono state 9.140. Ovvero 2.731,3 ogni 100mila abitanti. Nell'Aretino si registrano dati oltre la media per quanto riguarda frodi informatiche (21esimo posto), incendi (28esimo), reati legati alla droga (30esimo posto), furti nei negozi (32esimo) e, anche se con meno vigore, per quanto riguarda i furti con destrezza (48esimo posto su 106) e le rapine (49esimo).

CONTESTO INTERNO

La Società ha per oggetto qualunque attività affine o connessa alla realizzazione, gestione e manutenzione di reti telematiche e progettazione, sviluppo, produzione, promozione, gestione e commercializzazione di servizi informatici, telematici, indirizzati prevalentemente a pubbliche amministrazioni. La Società, per la realizzazione dello scopo sociale, può operare in tutti i settori attinenti alla gestione dei servizi pubblici, nel rispetto dei principi della legislazione in materia, dalle norme attuative regionali e fatte salve le necessarie determinazioni da parte delle autorità competenti.

Nell'ambito di quanto sopra, la Società svolge le seguenti altre attività:

- la promozione e la realizzazione di progetti informatici-telematici innovativi, partecipando altresì a programmi di ricerca e sviluppo in collaborazione con enti pubblici;
- la progettazione, la costruzione, il riordino, la gestione e la manutenzione di impianti e reti informatiche coerenti con lo scopo sociale, fornendo assistenza e formazione in tutti i processi tecnici inerenti l'interconnessione a mezzo reti telematiche - informatiche;
- lo sviluppo ed il commercio del software di base, standard ed applicativo;
- la raccolta, la conservazione, il trattamento e l'elaborazione di dati per la pubblica amministrazione;
- lo svolgimento di tutte le attività necessarie e/o connesse alla gestione tecnica, economica, finanziaria ed amministrativa dei servizi di cui sopra.

La Società può infine, ai fini del perseguimento del proprio scopo sociale, compiere qualsiasi operazione finanziaria, industriale, mobiliare ed immobiliare, utile o opportuna, a giudizio dell'Amministratore Unico, ivi compresa l'utilizzazione di sovvenzioni da parte di soggetti pubblici e/o privati, di organizzazioni comunitarie ed internazionali, al fine del conseguimento dell'oggetto sociale.

La Società ha, inoltre, come scopo:

- ricerca, sviluppo, realizzazione, installazione, commercializzazione e gestione di sistemi di telecomunicazioni di ogni genere;
- la vendita, la locazione ed il noleggio di macchine per l'elaborazione dati, hardware e software, compresi componenti ed accessori, nonché la fornitura di materiale ausiliario, ivi compresa la locazione di impianti ed attrezzature per video-conferenze e di impianti telematici in genere;
- le altre attività economiche accessorie, purché direttamente strumentali alle attività e/o alle funzioni amministrative degli enti locali soci coerenti con l'oggetto sociale fondamentale e comunque di entità economica non prevalente in relazione ai servizi pubblici locali gestiti in auto produzione, ai sensi e per gli effetti delle normative vigenti e delle direttive comunitarie di riferimento.

La Società può assumere e concedere agenzie, commissioni, rappresentanze, con o senza depositi e mandati; acquistare, utilizzare e trasferire brevetti e altre opere dell'ingegno umano, compiere ricerche di mercato, di *customer satisfaction* ed elaborazione di dati per conto proprio e per conto di terzi, concedere ed ottenere licenze di sfruttamento commerciale nonché compiere tutte le operazioni commerciali (anche di import-export), finanziari, mobiliari e immobiliari, necessarie o utili per il raggiungimento degli scopi sociali.

Tutte le predette attività debbono essere svolte nei limiti e nel rispetto delle norme che ne disciplinano l'esercizio, con particolare riferimento al rispetto dei fini istituzionali e dei criteri di efficienza ed efficacia previsti dalle vigenti disposizioni pubblicistiche, conformandosi ai principi di pubblico interesse nella gestione dei pubblici servizi, nonché alle specifiche normative settoriali che li disciplinano e alle disposizioni in materia di carta dei servizi pubblici. In particolare, le attività di natura finanziaria dovranno comunque risultare conformi anche alle specifiche del modello societario *in house providing*, come desumibili dalle normative e dalle direttive comunitarie vigenti di tempo in tempo.

La Società attualmente è un personale con una dotazione di azioni proprie, così ripartita

PROVINCIA DI AREZZO	183.750,00	83,73
AZIONI PROPRIE	35.700,00	16,27
TOTALE	219.450,00	100,00

La Provincia di Arezzo esercita su Ar.Tel. S.p.A. il controllo analogo proprio delle società *in house* così come definite dalla normativa comunitaria.

La Società è amministrata da un Amministratore Unico, così come disposto dal D.Lgs. n. 175/2016.

Secondo il Regolamento della Provincia di Arezzo, i consiglieri/amministratori durano in carica per il periodo di due esercizi e salvo circostanze eccezionali non sono rieleggibili. L'Amministratore Unico è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, essendo ad esso demandato di compiere tutti gli atti opportuni per l'attuazione dell'oggetto sociale, esclusi soltanto quelli che per legge ed in base allo statuto, siano riservati all'Assemblea dei soci.

All'Amministratore Unico, nominato dall'Assemblea, e alla persona designata a sostituirlo in caso di assenza o impedimento, è attribuita la rappresentanza sociale e legale anche in giudizio. Il Collegio Sindacale, eletto dall'Assemblea, nel rispetto degli equilibri di genere, è composto da tre sindaci effettivi e due supplenti. Si rimanda allo Statuto per maggiori dettagli. Il Revisore legale è un organo monocratico.

Per quanto riguarda le attività svolte dalla Società, queste sono regolate da contratti di servizio come modalità di affidamento di lavoro/progetti da parte della Provincia di Arezzo per circa l'80% del

fatturato della Società e per il rimanente 20% da parte dei Comuni del territorio e dei Consorzi di bonifica, sempre su progetti web e gis, oltre che per la manutenzione del sistema.

Le aree di attività della Società, riferita ai servizi della Provincia, e alla attività dei Comuni / Regione Toscana, sono

- Edilizia ed Impianti
- Trasporti
- Viabilità LL.PP.
- Pianificazione territoriale
- Protezione Civile
- Istruzione

Inoltre, la Società gestisce per la Provincia di Arezzo i sistemi di telecomunicazione con la rete RTRT, lo sviluppo e manutenzione del portale ufficiale, gli applicativi di pubblicazione online dei dati, mentre ai Comuni viene dato il supporto tecnico e realizzazione sistemi per attività di informatizzazione di procedure, realizzazione di dati, servizi di posta elettronica e altro. La Società non ha quote di altre società.

RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA (RPCT)

L'Amministratore unico della Società ha nominato il Responsabile della Prevenzione e della Corruzione nella persona dell'Ing. Giovanni Tomassini che predispose il Piano triennale di prevenzione della corruzione e della trasparenza che sottopone al Consiglio di Amministrazione per l'approvazione solitamente entro il 31 gennaio di ogni anno.

Il ruolo del Responsabile della prevenzione della corruzione è stato rafforzato dalle novità, in materia di trasparenza, introdotte dal D.Lgs. n. 97/2016 in quanto unisce i due incarichi, quello di RPC e RT, prevedendo che vengano riconosciuti poteri e funzioni idonei allo svolgimento della propria attività in autonomia ed effettività. Il Piano è pubblicato sul sito web di Ar.tel. S.p.A. nella sezione Società Trasparente nella sottosezione Disposizioni Generali.

REFERENTI

Nella consapevolezza che la prevenzione dei fenomeni corruttivi non possa che essere il frutto di una necessaria interazione delle risorse, delle competenze e delle capacità di ognuno, tutto il personale, in relazione alle proprie competenze, è tenuto alla conoscenza del Piano Triennale di Prevenzione della Corruzione e della Trasparenza e deve darvi esecuzione.

Tutti i dipendenti partecipano al processo di gestione del rischio, osservano le misure contenute nel Piano segnalando le eventuali fattispecie di illecito e le personali situazioni di conflitto di interesse.

La violazione delle misure di prevenzione previste dal Piano costituisce oltre che l'eventuale

commissione di un reato:

- illecito disciplinare quando commessa da dipendenti della Società;
- grave inadempimento contrattuale, quando commessa da collaboratori, da consulenti e fornitori che svolgono attività in maniera rilevante o continuativa per conto o nell'interesse della Società. In forza di tale inadempimento, la Società sarà legittimata a risolvere il contratto con gli stessi con effetto immediato, ai sensi e per gli effetti dell'art. 1456 del Codice Civile, salve le eventuali azioni per ulteriore danno;
- fonte di responsabilità ex articolo 2392 del Codice Civile per gli amministratori;
- fonte di responsabilità ex articolo 2407 del Codice Civile per i Sindaci;

Tutti i dipendenti mantengono comunque il personale livello di responsabilità per il verificarsi di fenomeni corruttivi in relazione ai compiti effettivamente svolti.

STATO DI ATTUAZIONE

Nell'anno di riferimento non sono state rilevate violazioni e/o irregolarità. L'attività di formazione e parziale monitoraggio è avvenuta anche durante la modalità lavorativa in smart working durante la quale non sono emerse particolari criticità. Al personale della società è stata inviata una copia del presente Piano al fine di reperire osservazioni utili all'approvazione di un testo che non rappresenti una mera formalità ma un impegno concreto e condiviso a favore della legalità.

In considerazione della totale assenza di fatti illeciti da segnalare, si può confermare in linea generale la valutazione delle attività a rischio corruzione dello scorso anno.

Si segnala che non sono pervenute osservazioni durante la fase di pubblicazione dell'avviso di aggiornamento del PTPCT per il triennio 2023-2025.

ATTIVITÀ A RISCHIO CORRUZIONE

L'Azienda ha individuato le attività di seguito descritte rientranti nelle cosiddette aree di rischio indicate nella legge n. 190/2012, art. 1, comma 16.

L'insieme dei processi considerati hanno evidentemente una diversa gradazione e, pertanto, al fine di predisporre i necessari protocolli occorrerà valutare la rischiosità intrinseca di ogni processo e la diversa esposizione dei vari uffici.

Convenzionalmente potranno individuarsi tre gradazioni per gli aspetti di cui sopra con le qualificazioni di: *elevata, media, scarsa*. In questa sezione per ogni tipologia di processo sarà individuato il livello e l'indicazione degli uffici esposti con l'individuazione, per ciascuno, del grado di esposizione.

AREA AFFIDAMENTO LAVORI, FORNITURE E SERVIZI:

Si tratta dell'affidamento a terzi (pubblici o privati) di forniture di beni o servizi.

- Rapporti con operatori economici

Attività: tutta quella attività di contatti con gli operatori economici in qualche modo interessati ad effettuare forniture di beni e servizi alla Società; si fa riferimento ai contatti con gli operatori economici sia durante la fase di ideazione e programmazione delle forniture, lavori, servizi, che in quelle successive di affidamento anche mediante procedure di evidenza pubblica ed esecuzione. Si tratta dell'attività di selezione e di gestione del processo di procurement di beni e servizi.

Dal momento che per la natura stessa della società (società *in house* che svolge servizi per conto dell'ente affidatario) questa attività è di scarsa entità pertanto il rischio associato può definirsi SCARSO. Si precisa che la maggior parte delle forniture e dei servizi viene fatto tramite mercato elettronico.

Uffici esposti al rischio: Ufficio Amministrazione

AREA PERSONALE:

Rientrano in quest'area le attività relative alla costituzione o modificazione di rapporti di lavoro autonomo o subordinato. Incarichi di collaborazione – Progressioni di carriera.

Attività: tutta l'attività relativa alla programmazione e attivazione di rapporti di lavoro autonomo o subordinato; è da far riferimento all'attività che precede la fase della programmazione e quella dell'attivazione di procedure di selezione. Sono altresì rilevanti i processi relativi a trasformazioni o modificazioni di rapporti già in essere con la Società.

Attività relativa al processo di selezione, assunzione, retribuzione e valutazione dei dipendenti e dei meccanismi di incentivazione del personale.

Sono da escludere, invece, per le particolari modalità formali di conduzione, le attività poste in essere per l'applicazione di sanzioni disciplinari.

Rischio: ELEVATO

Uffici esposti al rischio: Ufficio Amministrazione

CONTROLLI SULL'ESATTO ADEMPIMENTO E GESTIONE DELL'ESECUZIONE:

Attività: l'esatto adempimento delle obbligazioni dedotte in contratto è essenziale. È assolutamente necessario il controllo sulla qualità e quantità nonché sul rispetto dei termini di esecuzione.

Rischio: ELEVATO

Uffici esposti al rischio: AD

MISURE DI PREVENZIONE

Argomento del rischio	Misure di prevenzione	Tempi	Responsabili
Affidamento lavori, servizi e	Divieto del frazionamento del	In atti	Resp. Amm.

forniture:	valore d'appalto		
Affidamento lavori, servizi e forniture:	Redazione della documentazione d'appalto La documentazione di gara viene redatta da persona diversa da quella che autorizza l'atto.	In atti	Resp. Amm. per la documentazione Amministratore per l'autorizzazione
Affidamento lavori, servizi e forniture:	Garantire la partecipazione di più concorrenti, evitando requisiti di aggiudicazione troppo restrittivi e/o mirati. Privilegiare, ove possibile, il requisito dell'offerta "al massimo ribasso" nelle procedure di affidamento per prestazioni ove i criteri di qualità sono prestabiliti dall'Azienda.	In atti	Amministratore
Affidamento lavori, servizi e forniture:	Rotazione, nei limiti di legge, degli operatori economici da invitare alla presentazione delle offerte.	In atti	Resp. Amm.
Affidamento lavori, servizi e forniture:	Scadenziario dei contratti. Le proroghe di contratti ad esecuzione continuata sono possibili soltanto per oggettive necessità oppure qualora, almeno sei mesi prima della scadenza, sia avviata apposita procedura volta al prolungamento del contratto in essere.	In atti	Amministratore
Affidamento lavori, servizi e forniture:	Per affidamenti di importi fino a € 200.00 (iva esclusa), pagamento in contanti con fornitore scelto dal responsabile. Per affidamenti di importo compreso tra € 200 e € 500 (iva esclusa) obbligo, fatte	In atti	Resp. Amm.

	<p>salve eventuali motivazioni nei limiti di legge, di chiedere, almeno 3 preventivi tra gli operatori economici del settore, garantendone la rotazione, in funzione della disponibilità di mercato e della tipologia della prestazione. Per affidamenti superiori a € 500 (iva esclusa) obbligo di procedure di evidenza pubblica secondo quanto stabilito nel regolamento di contabilità della Provincia di Arezzo</p>		
--	--	--	--

Area Personale	Predisposizione di precise norme relative alla progressione di carriera del personale	In atti	Amministratore
Area Personale	Conferimento incarichi di collaborazione / incarichi professionali	In atti	Amministratore
Area Personale	Selezione mediante esamina annuale dei curricula, con valutazione della professionalità acquisita dalle precedenti esperienze maturate	In atti	Amministratore
Area Personale	Regolamento interno su assunzione e conferimento di incarichi pubblicato sul sito della Società	In atti	Amministratore

FORMAZIONE, CONTROLLO E PREVENZIONE DEL RISCHIO

Conformemente a quanto richiesto dalla legge n. 190 del 2012, la Società adotta misure finalizzate alla prevenzione della corruzione con riferimento sia alla fase di formazione che di attuazione delle

decisioni relative alle attività maggiormente esposte a rischio. Le singole attività a rischio di corruzione sono indicate ai paragrafi precedenti.

Coloro che partecipano alla formazione della volontà devono dichiarare l'inesistenza di conflitti di interesse, seppure potenziali; sussiste conflitto di interesse anche nel caso di rapporti negoziali privati tra Amministratore, dipendente e appaltatore sia in corso che esauriti da non oltre un triennio.

È richiesto a ciascun dipendente di segnalare le eventuali situazioni di conflitto di interesse esistenti con riferimento alle attività dallo stesso svolte e avendo riguardo anche a quanto previsto dagli artt. 6 e 7 del D.P.R. n. 62/2013 e dal codice disciplinare e dal codice di comportamento. La segnalazione deve essere redatta per iscritto e inviata al proprio Resp. di Area.

La società verifica l'insussistenza di ipotesi di inconferibilità ed incompatibilità degli incarichi degli organi amministrativi della Società ai sensi del D.Lgs. n. 39 del 2013.

L'accertamento avviene al momento del conferimento dell'incarico mediante dichiarazione sostitutiva di certificazione resa dall'interessato, pubblicata sul sito istituzionale della Società.

La Società adotta tutte le misure necessarie ad evitare l'assunzione di dipendenti pubblici, che negli ultimi tre anni abbiano esercitato poteri autoritativo o negoziali per conto di pubbliche amministrazioni, nei confronti della Società stessa. A tal fine la Società attua iniziative volte a garantire che: a) negli interpellati o comunque nelle varie procedure di selezione del personale sia inserita la condizione ostativa sopra indicata; b) i soggetti interessati presentino una dichiarazione di insussistenza di tale causa ostativa; c) sia svolta una specifica attività di vigilanza, eventualmente anche secondo modalità definite e su segnalazione di soggetti interni ed esterni.

I dipendenti, non solo quelli che svolgono attività potenzialmente a rischio di corruzione, segnalano al Responsabile Area di appartenenza qualsiasi anomalia accertata indicando, se a loro conoscenza, le motivazioni della stessa.

L'Amministratore può tenere conto di segnalazioni provenienti da eventuali portatori di interessi esterni alla Società, purché non anonime e sufficientemente circostanziate, che evidenzino situazioni di anomalia e configurino il rischio del verificarsi di fenomeni corruttivi.

Nel 2015 la Società ha attivato un account di posta elettronica (anticorruzione@ar-tel.it), presso il quale i componenti dell'organizzazione potranno segnalare fatti rilevanti sotto il profilo disciplinare o penale. L'identità del segnalante non può essere rivelata (ai sensi dell'art.1, comma 51, Legge 190/2012).

Le segnalazioni che dovessero risultare assolutamente infondate daranno luogo, ove applicabili, a procedimenti sanzionatori previsti dalla legge. Tutti coloro i quali intendano corrispondere mediante mail, hanno l'obbligo di inserire nel corpo della e-mail, ovvero della nota spedita via posta tradizionale, apposita dichiarazione al trattamento dei dati personali a norma del T.U. 196/03 (Codice sulla privacy). L'Azienda è intenzionata a pianificare specifiche attività formative rivolte al personale dipendente, in

materia di anticorruzione e trasparenza. Gli interventi formativi avranno l'obiettivo di far conseguire ai dipendenti conoscenza dei contenuti, finalità e adempimenti conseguenti relativi a:

- piano triennale anticorruzione e trasparenza;
- codice di comportamento dei dipendenti;
- trasparenza e anticorruzione;

L'Azienda concorderà un aggiornamento continuo sulle misure e sulle disposizioni applicabili nei suddetti ambiti. I Responsabili di Area, coadiuvati dal Responsabile della prevenzione della corruzione, individueranno il personale impiegato nelle attività a rischio, anche ai fini della partecipazione ai suddetti percorsi formativi.

Il CdA del 26 maggio 2016 ha approvato il Codice di Comportamento dei dipendenti che è stato pubblicato nel sito della Società e trasmesso a tutti i dipendenti. Gli obblighi di condotta previsti dal suddetto Codice sono estesi, per quanto compatibili, a tutti i collaboratori e alle imprese che forniscono alla Società beni o servizi.

Per la contestazione, l'accertamento delle infrazioni e l'applicazione di sanzioni disciplinari restano validi i poteri già conferiti, nei limiti delle rispettive deleghe e competenze, al management della Società. Il sistema sanzionatorio della Società trova la sua primaria fonte nell'art. 225 Provvedimenti disciplinari e seguenti del contratto COMMERCIO TERZIARIO - APPRENDISTI ASS. 7/2004

Nell'applicazione del provvedimento sanzionatorio, vengono presi in considerazione i seguenti aspetti:

- l'intenzionalità del comportamento;
- il grado di negligenza, imprudenza o imperizia;
- il comportamento complessivo del dipendente anche in relazione a eventuali precedenti disciplinari di portata simile;
- le mansioni svolte dal lavoratore e la posizione dallo stesso ricoperta;
- il coinvolgimento di altre persone;
- la rilevanza o meno esterna in termini di conseguenze negative per la Società del comportamento illecito.

Le sanzioni che si possono applicare sono le seguenti

- biasimo inflitto verbalmente per le mancanze lievi;
- biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui al precedente punto 1);
- multa in misura non eccedente l'importo di 4 ore della normale retribuzione di cui all'art. 193;
- sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;
- licenziamento disciplinare senza preavviso e con le altre conseguenze di ragione e di legge.

È fatta in ogni caso salva la facoltà per la Società di agire per il risarcimento dei danni

L'Azienda, in ragione delle ridotte dimensioni e del numero limitato di personale operante all'interno delle aree di competenza, ritiene che la rotazione del personale causerebbe inefficienza e inefficacia

dell'azione amministrativa tale da precludere in alcuni casi la possibilità di erogare in maniera ottimale i servizi. Pertanto, l'Azienda ritiene opportuno non applicare nessuna rotazione del personale.

SEGNALAZIONI DI ILLECITI E TUTELA DEL SEGNALANTE (*WHISTLEBLOWING*)

L'introduzione nell'ordinamento nazionale di un'appropriata tutela del segnalante (pubblico o privato) che segnala condotte illecite in ambito lavorativo deriva dalla normativa internazionale.

L'art. 1, co. 51, della legge 6 novembre 2012, n. 190 ha inserito l'art. 54-bis all'interno del d.lgs.

30 marzo 2001 n. 165 «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche». Tale norma prevede un regime di tutela del dipendente pubblico che segnala condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro.

Il citato art. 54-bis è stato modificato, in seguito, dal decreto legge 24 giugno 2014, n. 90, convertito nella legge 11 agosto 2014, n. 114 che ha disposto che sia anche ANAC il soggetto destinatario delle segnalazioni di whistleblowing.

L'ultimo intervento normativo in materia è stato dettato dalla legge 30 novembre 2017 n. 179, «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», il cui art. 1 modifica integralmente l'art. 54 -bis prevedendo: l'ampliamento dell'ambito soggettivo di applicazione, la valorizzazione del ruolo del Responsabile della prevenzione della corruzione e della trasparenza (RPCT) nella gestione delle segnalazioni, il sistema generale di tutela e protezione del segnalante che comprende la garanzia di riservatezza sull'identità, la protezione da eventuali misure ritorsive adottate dalle amministrazioni o enti a causa della segnalazione, nonché la qualificazione della segnalazione effettuata dal whistleblower come "giusta causa" di rivelazione di un segreto d'ufficio, aziendale, professionale, scientifico o industriale o di violazione del dovere di lealtà e fedeltà.

Ai sensi della legge n. 179\2017, ANAC ha adottato il seguente provvedimento con Delibera n. 469 del 9 giugno 2021: Schema di Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing) che superano le precedenti adottate con Determinazione n. 6 del 28 aprile 2015 (e i relativi allegati), i cui effetti si intendono cessati.

Le vigenti Linee Guida hanno un duplice obiettivo: dal un lato quello di fornire indicazioni sull'applicazione della normativa e sono rivolte alle pubbliche amministrazioni e agli altri enti indicati dalla legge contenendo anche indicazioni utili per i possibili "segnalanti"; dall'altro sono, altresì, volte a consentire alle amministrazioni e agli altri soggetti destinatari delle stesse di adempiere correttamente agli obblighi derivanti dalla disciplina di protezione dei dati personali (Regolamento (UE) 2016/679 del Parlamento europeo e d.lgs. 30 giugno 2003, n. 196, adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il d.lgs. 10 agosto 2018, n. 101).

L'art. 54-bis, co. 2, del d.lgs. 165/2001, come modificato dall'art. 1 della l. 179, individua l'ambito soggettivo di applicazione della disciplina sulla tutela del dipendente che segnala condotte illecite. La nuova formulazione dell'art. 54-bis include espressamente, al comma 2, nella nozione di dipendente pubblico le seguenti tipologie di lavoratori: i dipendenti delle amministrazioni pubbliche di cui all'art. 1, comma 2 del D.Lgs. n. 165 del 2001; i dipendenti degli enti pubblici economici; i dipendenti di enti diritto privato sottoposti a controllo pubblico ai sensi dell'articolo 2359 del codice civile; i lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica (la disciplina sulla tutela si applica a tali soggetti solo nel caso in cui le segnalazioni da essi effettuate riguardino illeciti o irregolarità relativi all'amministrazione per la quale l'impresa opera).

Ai fini dell'applicazione della disciplina del whistleblowing sono considerate le segnalazioni di condotte illecite effettuate solo da questi soggetti come previsto dal co. 1 dell'art. 54-bis.

Le segnalazioni di condotte illecite di cui il dipendente sia venuto a conoscenza in ragione del rapporto di lavoro, come previsto dall'art 54-bis (art. 1, co. 1), possono essere inviate, a discrezione del *whistleblower*, al RPCT dell'amministrazione ove si è verificata la presunta condotta illecita o ad ANAC. Il dipendente può anche valutare di inoltrare una denuncia «all'autorità giudiziaria ordinaria o a quella contabile». Tuttavia, è raccomandato dalla stessa ANAC che sia favorito, in prima istanza, il canale interno attraverso l'inoltro della segnalazione al RPCT.

Ai sensi di legge, l'unico soggetto che, all'interno dell'amministrazione può ricevere le segnalazioni di *whistleblowing*, con le connesse garanzie di protezione del segnalante, è il RPCT.

La legge 179 assegna al RPCT un ruolo fondamentale nella gestione delle segnalazioni. Il RPCT oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari a una prima "attività di verifica e di analisi delle segnalazioni ricevute", da ritenersi obbligatoria in base al co. 6, dell'art. 54-bis³², pena le sanzioni pecuniarie dell'Autorità (co. 1 e 6, art. 54-bis). Il RPCT è pertanto il soggetto legittimato, per legge, a trattare i dati personali del segnalante e, eventualmente, a conoscerne l'identità.

Pertanto, nel caso di segnalazioni destinate unicamente al superiore gerarchico il whistleblower non sarà tutelato ai sensi dell'art. 54-bis.

Per quanto riguarda le "comunicazioni di misure ritorsive" la norma prevede, invece, che esse siano trasmesse esclusivamente ad ANAC (art 54-bis, art. 1, co. 1). Nel caso in cui la comunicazione di misure ritorsive pervenga al RPCT dell'amministrazione ove le stesse si sono verificate, il RPCT offre il necessario supporto al segnalante rappresentando che la comunicazione deve essere inoltrata ad ANAC al fine di ottenere le tutele previste dall'art. 54-bis.

Perché al segnalante possa accordarsi la tutela prevista dall'art. 54-bis i presupposti sono i seguenti:

- il segnalante deve rivestire la qualifica di "dipendente pubblico" o equiparato;
- la segnalazione deve avere ad oggetto "condotte illecite"; - il dipendente deve essere venuto a conoscenza di tali "condotte illecite" "in ragione del proprio rapporto di lavoro";
- la segnalazione deve essere effettuata "nell'interesse all'integrità della pubblica amministrazione";
- la segnalazione deve essere inoltrata ad almeno uno delle quattro tipologie di destinatari indicati nell'art. 54-bis, co. 1 (RPCT, ANAC, Autorità giudiziaria ordinaria o contabile).

Per i pubblici ufficiali e gli incaricati di pubblico servizio che hanno un obbligo di denuncia, in virtù di quanto previsto dal combinato disposto dell'art. 331 c.p.p. e degli artt. 361 e 362 c.p., la segnalazione di cui all'art. 54-bis indirizzata al RPCT o ad ANAC non sostituisce, laddove ne ricorrano i presupposti, quella all'Autorità giudiziaria. Si rammenta che l'ambito oggettivo degli artt. 361 e 362 c.p., disponendo l'obbligo di denunciare soltanto reati (procedibili d'ufficio), è più ristretto di quello delle segnalazioni effettuabili dal whistleblower che può segnalare anche illeciti di altra natura.

I fatti illeciti oggetto delle segnalazioni *whistleblowing* comprendono non solo le fattispecie riconducibili all'elemento oggettivo dell'intera gamma dei delitti contro la pubblica amministrazione di cui al Titolo II, Capo I, del codice penale, ma anche tutte le situazioni in cui, nel corso dell'attività amministrativa, si riscontrino comportamenti impropri di un funzionario pubblico che, anche al fine di curare un interesse proprio o di terzi, assuma o concorra all'adozione di una decisione che devia dalla cura imparziale dell'interesse pubblico.

Si ribadisce che secondo l'art. 54-bis, le condotte illecite segnalate devono riguardare situazioni, fatti, circostanze, di cui il soggetto sia venuto a conoscenza «in ragione del rapporto di lavoro» precisando che la protezione prevista dall'art. 54-bis non opera nei confronti del pubblico dipendente che viola la legge al fine di raccogliere informazioni, indizi o prove di illeciti in ambito lavorativo

La segnalazione, oltre a indicare condotte illecite, deve essere fatta per la salvaguardia dell'interesse all'integrità della pubblica amministrazione.

La sussistenza di questo requisito viene accertata dal RPCT (o dall'ANAC) valutando la singola segnalazione che deve rilevare una lesione, un pregiudizio, un ostacolo, un'alterazione al corretto ed imparziale svolgimento di un'attività o di un servizio pubblico o per il pubblico, anche sotto il profilo della credibilità e dell'immagine dell'amministrazione.

Una volta valutata l'ammissibilità della segnalazione, quale segnalazione di *whistleblowing*, il RPCT avvia l'istruttoria interna sui fatti o sulle condotte segnalate.

Nel caso, invece, che a seguito dell'attività svolta, il RPCT ravvisi elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione.

L'ANAC ritiene che il termine per l'esame preliminare della segnalazione cui consegue l'avvio

dell'istruttoria debba essere di quindici giorni lavorativi che decorrono dalla data di ricezione della segnalazione.

Il termine per la definizione dell'istruttoria è di sessanta giorni che decorrono dalla data di avvio della stessa. Resta fermo che, laddove si renda necessario, l'Amministratore Unico può autorizzare il RPCT ad estendere i predetti termini fornendo adeguata motivazione.

Si ricorda che non spetta al RPCT accertare le responsabilità individuali qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dall'amministrazione oggetto di segnalazione, a pena di sconfinare nelle competenze dei soggetti a ciò preposti all'interno di ogni ente o amministrazione ovvero della magistratura.

Sebbene l'art. 54-bis non includa nel proprio campo di applicazione le segnalazioni anonime e cioè quelle del soggetto che non fornisce le proprie generalità, l'ANAC ritiene necessario che nel PTPCT o in altro apposito atto organizzativo vengano registrate le segnalazioni anonime e le segnalazioni di soggetti estranei alla p.a. pervenute attraverso i canali dedicati al whistleblowing.

Il sistema di protezione che la Legge n.179/2017 riconosce al *whistleblower* si compone di tre tipi di tutela:

- la tutela della riservatezza dell'identità del segnalante e della segnalazione;
- la tutela da eventuali misure ritorsive o discriminatorie eventualmente adottate dall'ente a causa della segnalazione effettuata;
- l'esclusione dalla responsabilità nel caso in cui il *whistleblower* (nei limiti previsti dall'art. 3, l. 179) - sia in ambito pubblico (ex art. 54-bis, d.lgs. 165/2001) che privato (ex art. 6d.lgs. 231/2001) - sveli, per giusta causa, notizie coperte dall'obbligo di segreto d'ufficio, aziendale, professionale, scientifico o industriale (artt. 326, 622, 623 c.p.) ovvero violi l'obbligo di fedeltà (art. 2105 c.c.).

Il comma 3 dell'art. 54-bis impone all'amministrazione, che riceve e tratta le segnalazioni, di garantire la riservatezza dell'identità del segnalante. Tale divieto è da riferirsi non solo al nominativo del segnalante ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, nella misura in cui il loro disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante. Ciò anche al fine di evitare l'esposizione dello stesso a misure ritorsive che potrebbero essere adottate a seguito della segnalazione all'interno dell'ente; pertanto la segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della legge 7 agosto 1990, n. 241 «Nuove norme sul procedimento amministrativo» e all'accesso civico generalizzato di cui all'art. 5, co. 2, del d.lgs. 33/2013.

La segnalazione non è più considerata sottratta all'accesso ai sensi del co. 4 dell'art. 54-bis nel caso in

cui la segnalazione venga trasmessa anche a soggetti diversi da quelli indicati dalla legge, per questo, l'identità del segnalante sia stata svelata.

Si applicheranno quindi le discipline delle singole tipologie di accesso (a seconda dei casi, documentale, civico o generalizzato). Sarà quindi compito dell'amministrazione bilanciare gli interessi contrapposti e valutare, previa interlocuzione con i controinteressati, tra cui il segnalante, se concedere o meno l'accesso alla segnalazione secondo i principi e limiti previsti dal d.lgs. 33 del 2013 o la l. 241 del 1990. Anche la normativa di protezione dei dati prevede una specifica disposizione a tutela dell'riservatezza dell'identità del segnalante. Il legislatore ha, infatti, introdotto, con il d.lgs. 10 agosto 2018, n. 10121 di recepimento del Regolamento (UE) n. 2016/679, l'art. 2-undecies nel d.lgs. 30 giugno 2003, n. 196. La norma richiamata stabilisce che nell'ambito di una segnalazione whistleblowing, il soggetto segnalato, (cfr. § 3.5 del Regolamento) presunto autore dell'illecito, con riferimento ai propri dati personali trattati dall'Amministrazione, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) n. 2016/679, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante. In tal caso, dunque, al soggetto interessato (segnalato) è preclusa la possibilità di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della Privacy (ai sensi dell'art. 77 del Regolamento (UE) n. 2016/679). Resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di esercitare i propri diritti con le modalità previste dall'art. 160 d.lgs. n. 196/2003.

È bene precisare che anche i dati relativi ai soggetti segnalati, in quanto interessati, sono comunque tutelati dalla disciplina in materia dei dati personali. Al fine di evitare la circolazione di informazioni personali, non solo verso l'esterno, ma anche all'interno degli uffici dell'amministrazione in capo a soggetti non autorizzati al trattamento dei dati, si provvederà ad una più idonea configurazione dei sistemi di protocollo informatico.

Nell'ambito del procedimento disciplinare attivato dall'amministrazione contro il presunto autore della condotta segnalata, l'identità del segnalante può essere rivelata solo dietro consenso di quest'ultimo. Nel caso in cui l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare, l'ente non potrà procedere con il procedimento disciplinare se il segnalante non acconsente espressamente alla rivelazione della propria identità

La legge prevede che *il whistleblower* non possa essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro. L'adozione di misure discriminatorie deve essere comunicata ad ANAC per gli accertamenti che la legge le attribuisce e per l'eventuale irrogazione della sanzione amministrativa al responsabile, come previsto dalla legge. Per misura ritorsiva non sono intesi solo gli atti e i provvedimenti ma anche i comportamenti o omissioni posti in essere dall'amministrazione nei confronti del dipendente/segnalante, volti a limitare e/o comprimere l'esercizio delle funzioni proprie

del lavoratore con intenti vessatori o comunque di peggiorare la situazione lavorativa. È necessario che il segnalante fornisca ad ANAC elementi oggettivi dai quali sia possibile dedurre la consequenzialità tra segnalazione effettuata e lamentata ritorsione.

Si evidenzia che, mentre nel primo comma dell'art. 54-bis si parla di misure ritorsive, nel comma 6il legislatore si riferisce a misure discriminatorie e nel comma 7 ad entrambe. Inoltre, nel comma 7 si specifica che gli atti ritorsivi o discriminatori adottati dall'amministrazione sono nulli.

Qualora venga accertata l'adozione di una misura ritorsiva o discriminatoria, ANAC applica al responsabile una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro (art. 1, co. 6, l. 179). Si precisa fin da ora che l'Autorità considera responsabile della misura ritorsiva il soggetto che ha adottato il provvedimento ritorsivo o comunque il soggetto a cui è imputabile il comportamento e/o l'omissione. La responsabilità si configura anche in capo al soggetto che ha suggerito o proposto l'adozione di una qualsiasi forma di ritorsione nei confronti del *whistleblower*, così producendo un effetto negativo indiretto sulla sua posizione (ad es. proposta di sanzione disciplinare).

La tutela prevista dall'art. 3, 1° comma, della legge 179, esclude che il *whistleblower* possa essere accusato di violazione del dovere di fedeltà e di lealtà per la "rivelazione e utilizzazione del segreto d'ufficio" (art. 326 cp), "rivelazione del segreto professionale" (art. 622 c.p.), "rivelazione dei segreti scientifici e industriali" (art. 623 cp) se avviene per "giusta causa" nel perseguire "l'interesse all'integrità della p.a. e alla prevenzione e repressione delle malversazioni nelle amministrazioni pubbliche e private».

Affinché il *whistleblower* possa usufruire delle tutele di cui all'art. 54-bis, devono essere soddisfatte le seguenti condizioni:

- il segnalante deve agire al fine di tutelare «l'interesse all'integrità delle amministrazioni, pubbliche e private, nonché alla prevenzione e alla repressione delle malversazioni» (art. 3, co. 1, l. 179);
- il segnalante non deve aver appreso la notizia «in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata» (art. 3, co. 2, l. 179);
- le notizie e i documenti, oggetto di segreto aziendale, professionale o d'ufficio, non devono essere rivelati «con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito» (art. 3, co.3, l. 179) e, in particolare, la rivelazione non deve avvenire al di fuori del canale di comunicazione specificamente predisposto per le segnalazioni.

In assenza di tali presupposti, l'aver fatto una rivelazione di fatti illeciti in violazione degli artt. 326, 622, 623 c.p.) e dell'art. 2105 c.c. è fonte di responsabilità civile e/o penale.

Per specifica previsione normativa (co. 9, art. 54-bis) 28 le tutele previste dall'art. 54-bis nei confronti del segnalante cessano in caso di sentenza, anche non definitiva di primo grado, che accerti nei

confronti dello stesso la responsabilità penale per i reati di calunnia o diffamazione o comunque per reati connessi alla denuncia, ovvero la sua responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o per colpa. Nel caso in cui la sentenza di primo grado, sfavorevole per il segnalante, non venga confermata nei successivi gradi di giudizio, sarà applicabile, sia pur tardivamente, la protezione del segnalante prevista dall'art. 54-bis per le eventuali ritorsioni subite a causa della segnalazione.

Nel processo di gestione delle segnalazioni, si distinguono i seguenti profili:

- Segnalante: soggetto che ha inviato la segnalazione di *whistleblowing*;
- RPCT: Responsabile Prevenzione della Corruzione e Trasparenza nominato dall'Ente.
- Custode dell'Identità: coincide con il RPCT

Per le segnalazioni di condotte illecite, la Società attiverà e pubblicherà un portale specifico che rispetta le prescrizioni della Legge n. 179/2017 e del Regolamento (UE) n. 2016/679 in termini di metodo di presentazione delle segnalazioni e di garanzia di riservatezza del segnalante; sarà conforme quindi a quanto disposto dall'ANAC nelle Linee Guida di cui alla Delibera n. 469 del 09.06.2021.

Il link di accesso al suddetto portale sarà pubblicato nella sezione "Società trasparente" del sito della Società e come indicato nelle citate Linee Guida ANAC verrà segnalato anche nell'homepage del sito istituzionale di Ar.tel. S.p.A.

OBBLIGHI DI TRASPARENZA

La Trasparenza è una misura di estremo rilievo e fondamentale per la prevenzione della corruzione. Essa è posta al centro di molte indicazioni e orientamenti internazionali in quanto strumentale alla promozione dell'integrità, allo sviluppo della cultura della legalità in ogni ambito dell'attività pubblica. Infatti proprio la Legge n. 190/2012 individua nel principio di trasparenza un valido strumento di prevenzione e di contrasto alla corruzione. Importanti innovazioni sono state apportate dal D.Lgs. 97/2016 in merito agli ambiti soggettivi di applicazione.

Le misure adottate per la Trasparenza e conseguentemente per la prevenzione della Corruzione costituiscono obiettivi della Performance.

In ottemperanza alla nuova normativa in merito agli obblighi di pubblicazione, l'ANAC ha formulato "Le Prime Linee Guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal D.Lgs. n. 97/2016".

A seguito dell'entrata in vigore il 25 maggio 2018 del Regolamento (UE) 2016/679 per la Tutela dei Dati, la Società ha affidato l'incarico Responsabile della Protezione dei Dati (RPD) alla Società Esseti Servizi Telematici S.r.l. che si avvale dell'avvocato Flavio Corsinovi, così come pubblicato sul sito dell'Ente nella sezione Società Trasparente/ Disposizioni Generali.

In questo contesto, così come deliberato dal Consiglio d'Amministrazione, la Società provvederà all'adozione di linee guida sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel D.Lgs. 33/2013 alla luce delle previsioni del Regolamento (UE) 679/2016 in materia di protezione dei dati personali delle persone fisiche.

IL RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA:

- svolge stabilmente un'attività di controllo sull'adempimento da parte dell'amministrazione degli obblighi di pubblicazione previsti dalla normativa vigente, assicurando la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate;
- è Responsabile del reperimento dei dati e della loro pubblicazione nella sezione Amministrazione Trasparente;
- controlla e assicura la regolare attuazione dell'istituto dell'accesso civico (art. 43 co. 4 D.Lgs. 33/2013).

Il sito internet istituzionale della Società (www.ar-tel.it) costituisce il mezzo primario di comunicazione e il più accessibile attraverso il quale si può garantire un'informazione trasparente, pubblicizzare e consentire l'accesso ai servizi, consolidare la propria immagine istituzionale.

In conformità con la normativa vigente, sul sito web della Società, nella homepage, è presente apposita sezione denominata "*Società trasparente*" suddivisa in sottosezioni secondo quanto previsto dal D.Lgs. n. 33/2013, come modificato dal D.Lgs. n. 97/2016.

La pubblicazione on line delle informazioni di cui al paragrafo precedente è effettuata in coerenza con quanto riportato nel Decreto Trasparenza (il D.Lgs. n. 33/2013, come modificato dal D.Lgs. n. 97/2016), e secondo le caratteristiche istituzionali e organizzative dell'Ente, con particolare riferimento a:

- aggiornamento e visibilità dei contenuti (tempestività)
- chiarezza e accessibilità
- classificazione e semantica
- formati e contenuti aperti

fatto salvo il rispetto delle normative specifiche in materia di riservatezza dei dati personali.

Posta elettronica certificata

La Società Ar.tel. S.p.A. ha pubblicato sul sito istituzionale l'indirizzo PEC ar-tel@pec.it. La posta ricevuta nella casella PEC viene gestita dall'apposito ufficio.

La PEC viene utilizzata ordinariamente per la trasmissione di documenti relativi all'attività istituzionale dell'Ente.

Accesso civico:

La tutela del diritto di accesso civico è disciplinata dalle disposizioni di cui dal D.Lgs. n. 33/2013. Il D.Lgs. n. 97/2016 ha introdotto accanto a quello già disciplinato, il diritto di chiunque di accedere a dati e documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione di cui al D.Lgs. n. 33/2013, (*accesso generalizzato*) nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti e dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'art. 5 bis, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

Ciò in attuazione del principio di trasparenza che il novellato articolo 1, comma 1, del decreto trasparenza ridefinisce come accessibilità totale dei dati e dei documenti detenuti dalle pubbliche amministrazioni non più solo finalizzata a "favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche", ma soprattutto, e con una modifica assai significativa, come strumento di tutela dei diritti dei cittadini e di promozione della partecipazione degli interessati all'attività amministrativa. L'intento del legislatore è ancor più valorizzato in considerazione di quanto già previsto nel co. 2 dell'art. 1 del decreto trasparenza secondo cui la trasparenza è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, e integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino. La trasparenza diviene, quindi, principio cardine e fondamentale dell'organizzazione delle pubbliche amministrazioni e dei loro rapporti con i cittadini. L'accesso generalizzato non sostituisce l'accesso civico "semplice" previsto dall'art. 5, comma 1 del decreto trasparenza, e disciplinato nel citato decreto già prima delle modifiche ad opera del d.lgs. 97/2016. L'accesso civico rimane circoscritto ai soli atti, documenti e informazioni oggetto di obblighi di pubblicazione e costituisce un rimedio alla mancata osservanza degli obblighi di pubblicazione imposti dalla legge, sovrapponendo al dovere di pubblicazione, il diritto del privato di accedere ai documenti, dati e informazioni interessati dall'inadempienza. L'accesso generalizzato si delinea come autonomo ed indipendente da presupposti obblighi di pubblicazione e come espressione, invece, di una libertà che incontra, quali unici limiti, da una parte, il rispetto della tutela degli interessi pubblici e/o privati indicati all'art. 5 bis, commi 1 e 2, e dall'altra, il rispetto delle norme che prevedono specifiche esclusioni (art. 5 bis, comma 3). L'accesso generalizzato deve essere anche tenuto distinto dalla disciplina dell'accesso ai documenti amministrativi di cui agli articoli 22 e seguenti della Legge 7 agosto 1990, n. 241 (d'ora in poi "accesso documentale"). La finalità dell'accesso documentale ex L. 241/90 è, in effetti, ben differente da quella sottesa all'accesso generalizzato ed è quella di porre i soggetti interessati in grado di esercitare al meglio le facoltà - partecipative e/o oppositive e difensive - che l'ordinamento attribuisce loro a tutela delle posizioni giuridiche qualificate di cui sono titolari. La regola della generale accessibilità è temperata, però, dalla previsione di eccezioni poste a tutela

di interessi pubblici e privati che possono subire un pregiudizio dalla diffusione generalizzata di talune informazioni. Dalla lettura dell'art. 5 bis, co. 1, 2 e 3 del decreto trasparenza si possono distinguere due tipi di eccezioni, assolute o relative.

L'accesso generalizzato è escluso nei casi indicati al co. 3 dell'art. 5 bis, nei casi cioè in cui una norma di legge, sulla base di una valutazione preventiva e generale, per tutelare interessi prioritari e fondamentali, dispone sicuramente la non ostensibilità di dati, documenti e informazioni ovvero la consente secondo particolari condizioni, modalità e/o limiti. Solo una fonte di rango legislativo può giustificare la compressione del diritto a conoscere cui ora il nostro ordinamento è improntato. Dette esclusioni (eccezioni assolute) ricorrono in caso di

- Segreto di Stato o divieto di divulgazione;
- negli altri casi di divieto di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche modalità o limiti, inclusi quelli di cui all'art. 24, comma 1, della legge n. 241 del 1990.

Al di fuori dei casi sopra indicati, possono ricorrere, invece, limiti (eccezioni relative o qualificate) posti a tutela di interessi pubblici e privati di particolare rilievo giuridico elencati ai commi 1 e 2 dell'art. 5-bis del decreto trasparenza.

La richiesta d'accesso civico può essere avanzata da chiunque senza limitazioni, gratuitamente e non deve essere motivata. Va inoltrata al RPCT al seguente indirizzo di posta elettronica: info@ar-tel.it. Entro 30 giorni la Società deve inserire nel sito il documento e trasmetterlo al richiedente. Oppure può comunicargli l'avvenuta pubblicazione e fornirgli il link alla pagina web.