Determinazione dell'Amministratore Unico n. 01 del 14/01/2021

OGGETTO: PROCEDURE DI ACQUISIZIONE DI LAVORI, FORNITURE E SERVIZI SOTTO SOGLIA COMUNITARIA AI SENSI DELL'ART. 1 DELLA L. 120/2020 DI CONVERSIONE DEL S.L. 76/2020 PER L'ANNO 2021 – DETERMINA A CONTRARRE.

L'AMMINISTRATORE UNICO

Premesso che:

- con i contratti di servizio stipulati con il Comune di Casalecchio di Reno, Prot. n.ri 39448-39453-39451-39445 del 7/12/2017 è stata affidata alla società Adopera la gestione degli immobili, delle strade, della sosta a pagamento, del calore e pubblica illuminazione, Prot. 32519 del 30/10/2019 la gestione del verde e Prot. 34405 del 28/10/2018 la gestione dei servizi cimiteriali;

- che con i contratti di servizio stipulati rispettivamente con il Comune di Zola Predosa Prot. n. 37777 del 24/12/2019 e con il Comune di Monte San Pietro Prot. n. 4637 del 20/03/2019 è stata affidata alla società Adopera la gestione dei servizi cimiteriali;

- il D.Lgs n. 50/2016 e s.m.i. (Codice):

  - all'art. 95 stabilisce che prima dell'avvio delle procedure di affidamenti dei contratti pubblici (di lavori, servizi e forniture di beni) le amministrazioni aggiudicatrici, e quindi per analogia anche le società patrimoniali che fungono da stazioni appaltanti, determinano di contrarre in conformità alla propria organizzazione e/o regolamento;

  - all'art. 30, comma 1, stabilisce che l'affidamento e l'esecuzione di appalti di opere, lavori, servizi, forniture e concessioni garantisce la qualità delle prestazioni e si svolge nel rispetto dei principi di economicità, efficacia, tempestività e correttezza. Nell'affidamento degli appalti e delle concessioni, le stazioni appaltanti rispettano, altresì, i principi di libera concorrenza, non discriminazione, trasparenza, proporzionalità, nonché di pubblicità con le modalità indicate nel presente codice. Il principio di economicità può essere subordinato, nei limiti consentiti, ai criteri ispirati a esigenze sociali, nonché alla tutela della salute, dell'ambiente, del patrimonio culturale e alla promozione dello sviluppo sostenibile, anche dal punto di vista energetico;

- nel rispetto degli atti di programmazione dei singoli Comuni Soci e del Piano Operativo Aziendale, le stazioni appaltanti possono fare ricorso alle procedure di acquisto in economia nelle ipotesi tassativamente indicate all'art. 36 del Codice, ora art. 1 DL 120/2020, nonché delle ipotesi specificate in regolamenti o in atti amministrativi generali di attuazione emanati da ciascuna stazione appaltante con riguardo alle proprie specifiche esigenze, ai sensi dello stesso.

Richiamati:

- il "Regolamento per l'acquisizione di beni e servizi adottato con determina dell'Amministratore Unico n. 3 del 15/07/2016;

- il d.lgs 56/2017;

- il D.L. 32/2019 convertito in L. 55/2019;

- il D.L. 16 luglio 2020 n. 76, coordinato con la legge di conversione 11 settembre 2020, n. 120, recante: Misure urgenti per la semplificazione e l'innovazione digitale, che ha ridisegnato l'art. 36, comma 2 del Codice nel modo seguente:

N.	Importo dell'appalto	Modalità
1	- lavori fino a 150.000 euro - forniture e servizi fino a 75.000 euro - servizi di ingegneria e architettura, attività di progettazione di importo inferiore a 75.000 euro	Affidamento diretto
2	- lavori da 150.000 a 350.000 euro - servizi e forniture da 75.000 euro a soglia - servizi di ingegneria e architettura, attività di progettazione di importo da 75.000 euro a soglia	Procedura negoziata senza bando (art. 63 Codice) previa consultazione di almeno 5 operatori economici
3	-lavori da 350.000 a 1.000.000 di euro	Procedura negoziata senza bando (art. 63 Codice) previa consultazione di almeno 10 operatori economici
4	-lavori da 350.000 euro a soglia	Procedura negoziata senza bando (art. 63 Codice) previa consultazione di almeno 15 operatori economici

Considerato quanto disposto al comma 2 dell'art. 40 del D.Lgs 50/2016 e s.m.i. e quindi che a decorrere dal 18/10/2018 tutte le stazioni appaltanti devono utilizzare mezzi di comunicazione elettronica nell'ambito delle procedure di gara allo scopo di garantire l'integrità dei dati e la riservatezza delle offerte e delle domande di partecipazione.

Preso atto della ricognizione per l'anno 2021 sui fabbisogni di lavori, servizi e forniture per importi fino ad € 150.000,00, effettuata con i Direttori Tecnici Ing. Francesco M. Cellini in qualità di Coordinatore e Ing. Franco Spalazzese, ognuno per la propria specifica competenza.

Visto che dall'analisi dei bisogni espressi allo stato attuale non si prevede l'affidamento di forniture di beni e servizi di importi unitari al di sopra della soglia prevista dall'art. 35, lett. b) e c) del D.Lgs 50/2016 e nel caso, si provvederà con specifiche procedure rispettando i principi fissati per le fattispecie di volta in volta individuati ed approvati con atti dedicati.

Dato atto che l'art. 1, comma 7 del D.L. 95/2012 stabilisce che le stazioni appaltanti sono tenute ad approvvigionarsi di beni e di servizi attraverso gli strumenti di acquisto e di negoziazione messi a disposizione da Consip S.p.A. e dalle centrali di committenza regionali di riferimento costituite ai sensi dell'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296, relativamente alle seguenti categorie merceologiche: energia elettrica, gas, carburanti, combustibili per riscaldamento, telefonia fissa e telefonia mobile.

Verificato che come indicato all'art. 1, comma 7 del D.L. 95/2012, per alcuni servizi sono già state attivate o si attiveranno procedure obbligatorie di affidamento tramite adesione a convenzioni Consip S.p.A. o Intercent-ER (telefonia mobile, energia elettrica a servizio della P.I., buoni pasto, pulizie e fornitura carburante).

Dato atto che:

- per l'esecuzione di lavori e per la fornitura di beni e servizi nelle categorie merceologiche diverse da quelle di cui al D.L. 95/2012, per importi unitari al di sotto della soglia comunitaria, le società patrimoniali mantengono la facoltà di rivolgersi al mercato elettronico centrale o regionale;

- nel caso di attivazione di procedure autonome, con bando, lettera invito e/o indagine di mercato, espresse anche mediante ordine diretto del Responsabile del Procedimento, per l'acquisto di determinati beni e servizi di cui all'elenco che segue, per importi economici comunque non superiori

alla soglia dei 75.000,00 euro così come indicato all'art. 1 della L. 120/2020, si terrà conto per quanto possibile di quanto presente sul MEPA o in apposite convenzioni Consip-Intercent-ER:

- *manutenzione ordinarie immobili, automezzi e mezzi operativi;*
- *servizi di spurgo, pulizia in edifici comunali;*
- *servizi noleggio e manutenzione fotocopiatrici;*
- *fornitura materiale di consumo per ufficio (toner, cancelleria);*
- *acquisto hardware e software ed eventuali relativi garanzie;*
- *manutenzione hardware e software in uso;*
- *servizi di formazione professionale specifica (tecnica ed amministrativa);*
- *servizi di postalizzazione, pubblicazioni e altri documenti;*
- *servizi di spedizione on-line, postalizzazione senza affrancatura;*
- *fornitura attrezzatura per adeguamento a normativa di sicurezza negli ambienti di lavoro compreso vestiario e dotazioni dpi;*
- *fornitura piante e materiale per il verde pubblico eseguiti in economia diretta;*
- *fornitura di materiale per gli interventi stradali eseguiti in economia diretta;*
- *fornitura di altro materiale (falegnameria, ferramenta, elettrico, idraulica, etc.) per gli interventi in economia diretta;*
- *fornitura materiale di consumo per ufficio (toner, cancelleria);*
- *acquisto hardware e software ed eventuali relativi garanzie;*
- *servizio di sorveglianza/guardiania edifici;*
- *servizi tecnici specifici non rientranti nelle professionalità presenti in società (catastali, frazionamenti, rilievi, confinamenti, certificazioni, perizie, accertamenti di laboratorio);*
- *servizi di supporto al Rup (progettazioni, redazioni piani sicurezza, collaudi);*
- *abbonamenti a riviste specializzate;*

- per i contratti di manutenzione di impianti esistenti e già manutenuti da imprese specializzate e di comprovata professionalità, si provvede all'affidamento in via diretta dei servizi ex art. 1, comma 2 lett. a) l. 120/2020, a seguito di apposita negoziazione ed aggiornamento effettuata con i singoli operatori economici rispetto al rapporto qualità/prezzo:

- impianti elevatori – E.S.A. S.p.A. e StarLift S.r.l.;
- impianti antintrusione e rilevazione incendi - Eurosistemi S.r.l.;
- cancelli-porte scorrevoli-stanghe - Sorce & Vannini S.r.l.;
- impianti semaforici del territorio – FIS Fabbrica Italiana Semafori S.r.l.;
- gruppi elettrogeni e apparati diversi - P.T.F. S.r.l.;
- servizi di guardiania sede e garage Ronzani - La Patria S.r.l.;
- revisione periodica sala compressori – Ariac S.r.l.;
- videosorveglianza cimitero di Zola Predosa, STAC2000;
- sistema antincendio non ricompresi nel contratto del servizio integrato calore-IP – Sicura S.p.A.;
- montascale con piattaforma cimitero calderino – Giovanelli Patrizio;
- macchina fotocopiatrice – GM2 S.r.l. (noleggio);
- auto a metano – Car Server S.p.A. (noleggio);

per i quali si acquisiscono i singoli codici CIG ai sensi di quanto disposto dall'art. 3 della L. 136/2010;

- per i contratti di manutenzione/gestione/implementazione dei programmi informatici in uso e già manutenuti dalle imprese fornitrici, sono confermati gli affidamenti alle seguenti imprese, su disposizione dei singoli Responsabili di Servizio e che fa seguito ad apposita negoziazione, agli atti:

- Programma E-Solver – contabilità e fatturazione elettronica – Servizio Informatica srl;
- Programma di posta elettronica e conservazione – SAAGE srl;
- Programma ASP per paghe, presenze personale, cartelle integrative – Zucchetti spa;
- Programma Formula EDK informativo e modulistica - Myo srl;
- Programma GescliWeb - gestione interventi interni – Servizio Informatica srl;

- Programma BaseBear - gestione della manutenzione - BaseBear srl;
- Servizio di WiFi aziendale - 3Cime srl;
- Programma gestione dei servizi cimiteriali - Gruppo Marche informatica srl;
- Gestione Whistleblowing – Impresa DigitalPA srl;
- Programma Sicurweb - gestione della sicurezza sul lavoro – InfotelSistemi srl;
- Programma Primus – gestione contabilità llpp – Acca Software srl;
- Programma JProtocollo – gestione del protocollo – Municipia spa;

per i quali si sono acquisiti originariamente o si acquisiscono se necessario i singoli codici CIG ai sensi di quanto disposto dall'art. 3 della L. 136/2010.

Tenuto conto di quanto disposto dalla L. 89/2014: *"i Comuni non capoluogo di provincia procedono all'acquisizione di lavori, beni e servizi nell'ambito delle Unioni dei Comuni di cui all'articolo 32 del D.Lgs 267/2000, ove esistenti, ovvero costituendo un apposito accordo consortile tra i Comuni medesimi e avvalendosi dei competenti uffici anche delle Province, ovvero ricorrendo ad un soggetto aggregatore o alle Province, ai sensi della L. 56/2014. In alternativa, gli stessi Comuni possono acquisire beni e servizi attraverso gli strumenti elettronici di acquisto gestiti da Consip S.p.A. o da altro soggetto aggregatore di riferimento"*. L'ANAC non rilascia il codice identificativo gara (CIG) ai Comuni non capoluogo di provincia che procedano all'acquisizione di lavori, beni e servizi in violazione degli adempimenti previsti dal presente comma. Precisato che con decorrenza 1/11/2015 tale l'obbligo vige anche per i lavori pubblici.

Vista la convenzione tra l'Unione dei Comuni Valli del Reno, Lavino e Samoggia ed i Comuni di Casalecchio di Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa per l'acquisizione in forma associata di lavori, beni e servizi, approvata con delibera di Consiglio Comunale n. 104 del 18/12/2014, così come modificata ed aggiornata con delibera di Giunta dell'Unione n. 15 del 27/02/2017.

Dato atto che rimane immutata la facoltà di Adopera per affidamento lavori al di sotto di € 150.000,00 e per servizi e forniture al di sotto di € 75.000,00 di procedere in autonomia.

Richiamato l'art. 1, comma 130 della L. 145/2018 nella quale si prevede la modifica dell'art. 1, comma 450 della L. 296/2006 per i soli servizi e fornitura con innalzamento della soglia dell'affidamento diretto su ordine del Rup ad € 5.000 senza necessariamente ricorrere all'e-procurment e/o all'utilizzo delle piattaforme telematiche.

Ravvisata la propria competenza all'adozione della presente determinazione ai sensi del mandato ricevuto e di quanto disposto dall'art. 20 dello Statuto societario.

Visti:
- ✓ il D.Lgs 50/2016;
- ✓ il D.Lgs 56/2017;
- ✓ la L. 145/2018;
- ✓ il DL 32/2019;
- ✓ il D.P.R. 207/2010 per le parti attualmente in vigore;
- ✓ le linee Guida n. 4 ANAC in attuazione al D.Lgs 50/2016 per quanto in vigore;
- ✓ il Regolamento degli interventi in Economia adottato in data 15/07/2016 con determina n. 3 dell'Amministratore Unico;
- ✓ la Legge 30 dicembre 2018, n. 145 (Legge di Bilancio 2019);
- ✓ la L. 120/2020 di conversione del D.L. 76/2020;

DETERMINA

per le ragioni meglio espresse in premessa,

- **di dare corso** per l'anno 2021 all'acquisizione di lavori, servizi e forniture ai sensi dell'art. 1 del D.L. 16 luglio 2020 n. 76, coordinato con la legge di conversione 11 settembre 2020, n. 120 (affidamento diretto con ordine del Responsabile del Procedimento e/o procedura semplificata, ristretta e/o negoziata, con o senza bando di gara) nel rispetto dei principi stabiliti dallo stesso Decreto e previa verifica dell'esistenza e dell'economicità, alla data di avvio dei singoli procedimenti ovvero quella di affidamento, del prodotto/servizio sul mercato elettronico MEPA, di apposite convenzioni Consip e/o Intercent-ER:

- ✓ telefonia mobile, energia elettrica, buoni pasto, pulizie, fornitura carburante, manutenzione impianti semaforici, spazzatura neve e spargimento sale;
- ✓ manutenzione ordinarie immobili, automezzi e mezzi operativi;
- ✓ servizi di spurgo, pulizia in edifici comunali;
- ✓ servizi noleggio e manutenzione fotocopiatrici;
- ✓ fornitura materiale di consumo per ufficio (toner, cancelleria);
- ✓ acquisto hardware e software ed eventuali relativi garanzie;
- ✓ manutenzione hardware e software in uso;
- ✓ servizi di formazione professionale specifica (tecnica ed amministrativa);
- ✓ servizi di postalizzazione, pubblicazioni e altri documenti;
- ✓ servizi di spedizione on-line, postalizzazione senza affrancatura;
- ✓ fornitura attrezzatura per adeguamento a normativa di sicurezza negli ambienti di lavoro compreso vestiario e dotazioni dpi;
- ✓ fornitura piante e materiale per il verde pubblico eseguiti in economia diretta;
- ✓ fornitura di materiale per gli interventi stradali eseguiti in economia diretta;
- ✓ fornitura di altro materiale (falegnameria, ferramenta, elettrico, idraulica, etc.) per gli interventi in economia diretta;
- ✓ fornitura materiale di consumo per ufficio (toner, cancelleria);
- ✓ acquisto hardware e software ed eventuali relativi garanzie;
- ✓ servizio di sorveglianza/guardiania edifici;
- ✓ servizi tecnici specifici non rientranti nelle professionalità presenti in società (catastali, frazionamenti, rilievi, confinamenti, certificazioni, perizie, accertamenti di laboratorio);
- ✓ servizi di supporto al Rup (progettazioni, redazioni piani sicurezza, collaudi);
- ✓ abbonamenti a riviste specializzate;

- **di confermare** l'affidamento dei contratti di manutenzione ordinaria di impianti esistenti e già manutenuti da imprese specializzate e di comprovata professionalità, per le ragioni meglio illustrate in premessa, ed in particolare:

- impianti elevatori – E.S.A. S.p.A. e StarLift S.r.l.;
- impianti antintrusione e rilevazione incendi - Eurosistemi S.r.l.;
- cancelli-porte scorrevoli-stanghe - Sorce & Vannini S.r.l.;
- impianti semaforici del territorio – FIS Fabbrica Italiana Semafori S.r.l.;
- gruppi elettrogeni e apparati diversi - P.T.F. S.r.l.;
- servizi di guardiania sede e garage Ronzani - La Patria S.r.l.;
- revisione periodica sala compressori – Ariac S.r.l.;
- videosorveglianza cimitero di Zola Predosa, STAC2000;
- sistema antincendio non ricompresi nel contratto del servizio integrato calore-IP – Sicura S.p.A.;
- montascale con piattaforma cimitero calderino – Giovanelli Patrizio;
- macchina fotocopiatrice – GM2 S.r.l. (noleggio);
- auto a metano – Car Server S.p.A. (noleggio);

- **di confermare** gli affidamenti dei contratti di manutenzione/gestione/implementazione dei programmi informatici in uso e già manutenuti dalle imprese fornitrici, per le ragioni meglio illustrate in premessa, e in particolare:

- Programma E-Solver – contabilità e fatturazione elettronica – Servizio Informatica srl;
- Programma di posta elettronica e conservazione – SAAGE srl;
- Programma ASP per paghe, presenze personale, cartelle integrative – Zucchetti spa;
- Programma Formula EDK informativo e modulistica - Myo srl;
- Programma GescliWeb - gestione interventi interni – Servizio Informatica srl;
- Programma BaseBear - gestione della manutenzione - BaseBear srl;
- Servizio di WiFi aziendale - 3Cime srl;
- Programma gestione dei servizi cimiteriali - Gruppo Marche informatica srl;
- Gestione Whistleblowing – Impresa DigitalPA srl;
- Programma Sicurweb - gestione della sicurezza sul lavoro – InfotelSistemi srl;
- Programma Primus – gestione contabilità llpp – Acca Software srl;
- Programma JProtocollo – gestione del protocollo – Municipia spa;

considerando comunque gli elenchi esemplificativi rispetto alle attività svolte e che potrebbero subire variazioni nel caso fossero affidate alla Società attività diverse rispetto alle attualmente in carico;

- **di acquisire** i codici CIG relativi ad ogni fornitura e/o servizio in ottemperanza a quanto previsto all'art. 3 della L. 136/2010;

- **di stabilire che** per ogni procedura di acquisto mediante ordine del Responsabile del Procedimento si farà riferimento alla presente atto quale determinazione a contrarre mentre per ogni altra procedura i Direttori Tecnici o l'Amministratore Unico assumeranno di volta in volta atti dedicati;

- **di dare atto:**

- che la spesa per l'anno 2021 è prevista nel Piano Operativo Aziendale;
- che il responsabile del procedimento ai sensi dell'art. 3 della legge n. 241/1990 è il firmatario del presente atto;
- che il presente provvedimento ha validità dal momento della sua sottoscrizione;

- **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del D.Lgs 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del D.Lgs 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

Determinazione dell'Amministratore Unico n. 02 del 02/02/2021

OGGETTO: PRESA D'ATTO DELLA DELIBERA DI GIUNTA DELL'UNIONE DEI COMUNI VALLI DEL RENO LAVINO SAMOGGIA – SIA - AVENTE AD OGGETTO: "APPROVAZIONE DISPOSIZIONI PER GLI UTENTI IN MERITO ALL'UTILIZZO DOTAZIONI INFORMATICHE (DUDI)".

L'AMMINISTRATORE UNICO

Premesso che l'Unione dei Comuni Valli del Reno, Lavino e Samoggia ha intrapreso da tempo, nell'ambito degli obiettivi di cui alla convenzione associativa Rep. 19/2014 un percorso progressivo miglioramento degli standard di sicurezza informatica, finalizzato alla tutela di dati, sistemi e infrastrutture informatiche di Unione ed Enti afferenti;

Richiamati:

- l'art. 17 del Codice dell'Amministrazione Digitale, che attribuisce al Responsabile della Transizione Digitale anche i compiti di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture;

- la circolare Agid 18 Aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" che e sono finalizzati a rispettare tali misure come specificate nella versione 1.0 dell'allegato tecnico protocollato con numero 12165 del 21/12/2017 (e successive modificazioni), che verrà richiamato negli articoli seguenti.

- il Regolamento Europeo n. 2016/6798 sulla protezione dei dati (GDPR), che prevede in capo agli Enti obblighi specifici in materia di tutela dei dati personali, parte dei quali riguardano la tutela dei dati trattati con sistemi informatici che rappresentano, in ragione dei processi di digitalizzazione delle procedure avviati negli ultimi anni, una parte sempre più importante di tutti i dati trattati da un'amministrazione pubblica.

Dato atto che le misure di sicurezza informatica da un lato vengono garantite tramite dotazioni hardware e software che compongono l'infrastruttura di rete (datacenter esternalizzato, regole per l'acceso al dominio, firewall, software antivirus), ma anche da un corretto comportamento degli utenti che utilizzano gli strumenti informatici (personal computer desktop, notebook, smartphone, tablet) utilizzati per lo svolgimento della propria attività lavorativa;

Sottolineato che l'importanza di un corretto utilizzo di tali strumenti è emersa in modo ancora più marcato a seguito dell'avvio straordinario della modalità di lavoro in smart working, a causa della pandemia Covid-19, durante la quale ai dipendenti è stato concesso come previsto dalle normative emergenziali di utilizzare anche dotazioni personali e non necessariamente messe a disposizione da parte dell'amministrazione;

Ritenuto pertanto opportuno raccogliere le disposizioni per il corretto utilizzo di tali strumentazioni in un unico documento che raccolga e aggiorni le regole che nel corso degli anni sono state definite in materia dal Servizio Informatico Associato;

Visto il Documento per l'utilizzo delle dotazione informatiche predisposto dal Servizio Informatico Associato ed in particolare dal Responsabile tecnico in collaborazione con il Responsabile di Servizio/Responsabile della Transizione digitale, che si allega al presente atto quale parte integrante e sostanziale;

Sottolineato che:

- tale documento è stato avallato dal DPO (Data Prorection Officer/Responsabile Trattamento Dati), nominato ai sensi del GDPR;

- parte delle disposizioni contenute in tale documento, sono finalizzate al rispetto delle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare Agid 18 Aprile 2017, n. 2/2017 alle quali anche Adopera ha l'onere di uniformarsi;

Ritenuto opportuno aderire alle indicazioni contenute nel documento facendole proprie e assicurandosi che il personale della Società le applichi e le rispetti;

Dato atto infine che il Responsabile del procedimento, ai sensi dell'art. 3 della legge n. 241/1990 e della nomina Prot. n. 13588 del 23/04/2019 è il firmatario del presente provvedimento;

Visti:

- il D.Lgs. 165/2001;
- il vigente Statuto societario;

DETERMINA

✓ **di prendere atto** dei contenuti della Delibera della Giunta dell'Unione dei Comuni Valli del Reno Lavino e Samoggia n. 11 dell'1/02/2021, esecutiva, con la quale si approvano le "DISPOSIZIONI PER GLI UTENTI IN MERITO ALL'UTILIZZO DOTAZIONI INFORMATICHE (DUDI)";

✓ **di dare atto che:**

- la presa d'atto costituisce provvedimento di indirizzo per la Società e per i propri dipendenti;

- il presente provvedimento ha validità dal momento della sua sottoscrizione;

- copia del Regolamento, allegato alla presente determina quale parte integrante, viene trasmesso a tutti i dipendenti della Società;

- di dare atto che nel caso in cui al documento vengano apportate dal SIA modifiche e/o aggiornamenti necessari per contrastare l'insorgenza di nuovi rischi, le stesse saranno adottate anche dalla Società mediante apposito atto di aggiornamento;

✓ **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del D.Lgs 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del D.Lgs 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

UNIONE DEI COMUNI VALLI DEL RENO, LAVINO E SAMOGGIA

Servizio Informatico Associato

Comuni di Casalecchio di Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa

D.U.D.I.
Disposizioni per gli Utenti in merito all'Utilizzo delle Dotazioni Informatiche

Versione	1.0.1
Aggiornato il	25/01/2021

1. Premesse e finalità 3

2. Entrata in vigore delle Disposizioni e pubblicità 3

3. Ambiti di applicazione 4

4. Utilizzo del Personal Computer 4

5. Gestione delle password e degli account 5

6. Utilizzo delle periferiche, delle cartelle condivise e della rete informatica 6

7. Utilizzo di altri dispositivi elettronici 7

8. Utilizzo e conservazione dei supporti rimovibili 8

9. Gestione ed utilizzo della posta elettronica ed altri strumenti di condivisione documenti 9

10. Utilizzo e navigazione in Internet 11

11. Protezione antivirus 11

12. Servizi e procedure di assistenza informatica 12

13. Utilizzo delle stampanti e dei materiali di consumo 12

14. Partecipazioni a social media 13

15. Osservanza delle disposizioni in materia di Privacy 13

16. Accesso ai dati trattati dall'utente 14

17. Sistemi di controlli graduali 14

18. Modalità di Smart working 14

19. Sanzioni 15

TAVALAZZI PAOLO DI CESARE NOTAIO IN MALALBERGO

1. Premesse e finalità

L'Unione Reno Lavino Samoggia, i Comuni di Casalecchio di Reno, Monte San Pietro, Sasso Marconi, Valsamoggia e Zola Predosa e le Aziende AdOpera Srl e Azienda Servizi per la Cittadinanza InSieme AscInsieme (di seguito "**Titolari**") dispongono che al proprio interno vengano osservate le presenti Disposizioni per gli Utenti disciplinanti l'utilizzo delle Dotazioni Informatiche (di seguito "**DUDI**").

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer e device mobili (come tablet e smartphone tra gli altri) e l'incremento dell'attività lavorativa in modalità smart working, espongono i Titolari a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dei Titolari stessi.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, i Titolari adottano le presenti Disposizioni interne dirette ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico e ad informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo n. 2016/6798 sulla protezione dei dati (da ora in poi GDPR), nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del predetto regolamento, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, comma 3, dello Statuto dei lavoratori.

Tale documento sarà unico per tutti gli Enti dell'Unione in quanto la gestione delle dotazioni, degli strumenti, dei servizi informatici e della digitalizzazione della P.A. viene gestita in forma unitaria dal Servizio Informatico Associato SIA (di seguito "**SIA**") dell'Unione in forza della convenzione associativa Rep. 19/2014.

I contenuti del DUDI inoltre sono stati determinati anche in considerazione della Circolare AGID 18 Aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" e sono finalizzati a rispettare tali misure come specificate nella versione 1.0 dell'allegato tecnico protocollato con numero 12165 del 21/12/2017 (e successive modificazioni), che verrà richiamato negli articoli seguenti.

Considerato inoltre che i Titolari, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, possono mettere a disposizione dei propri collaboratori che ne necessitino per il tipo di funzioni svolte, telefoni cellulari, computer portatili, tablet e smartphone, ecc., sono state inserite di seguito alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2. Entrata in vigore delle Disposizioni e pubblicità

2.1 - Con l'entrata in vigore delle presenti Disposizioni tutte le prescrizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

2.2 - Copia del presente documento, anche per quanto prevede l'art.7 della Legge n. 300/1970 (Statuto dei lavoratori), verrà diffuso con le seguenti modalità:

a) neo assunti: allegato al contratto di lavoro;
b) altri dipendenti: trasmesso via email e sempre a disposizione sulla sezione del Servizio Personale Associato contenente tutti i documenti di interesse dei dipendenti;
c) soggetti esterni che erogano servizi a favore dei Titolari: allegato a contratti di appalto che implichino l'utilizzo e/o l'accesso alla infrastruttura dell'Unione;
d) soggetti esterni istituzionali (es Città Metropolitana, forze dell'ordine etc): mediante trasmissione via email;
e) soggetti non istituzionali (es associazioni, start up, tirocinanti o altri utenti sporadici) che per diversi motivi utilizzino dotazioni informatiche all'interno delle sedi dell'Unione: allegato a nuovi contratti/convenzioni e, negli altri casi, trasmesso via email;

Pertanto, le presenti Disposizioni entrano a far parte, per quanto occorra, del Codice disciplinare aziendale.

Tale documento entrerà in vigore in seguito alla sua approvazione da parte delle Giunte

3. Ambiti di applicazione

3.1 - Le disposizioni contenute in questo documento si applicano:

- a tutti i dipendenti, senza distinzione di ruolo e/o livello
- a tutti gli amministratori (Sindaco, Assessori, Consiglieri)
- a collaboratori e consulenti dei Titolari a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, prestatori d'opera intellettuale, prestatori di servizi etc.) che venissero autorizzati a far uso di strumenti tecnologici dei Titolari o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.

Pertanto, le disposizioni di seguito previste devono intendersi a carico di tutte le figure sopra elencate, ferma restando la necessità che se ne dia opportuna conoscenza con le modalità di cui al punto 2.2.

3.2 - Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, amministratore (Sindaco, Assessore, Consigliere), collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile esterno del trattamento" o "terzo", ai sensi dell'art. 4 comma 10 del GDPR, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale o a favore dei Titolari stessi.

3.3 - Per quanto attiene gli amministratori, si precisa che nei loro confronti non valgono le disposizioni che secondo la normativa possono essere applicate solo in quanto collegate allo status di dipendente, tra cui si evidenziano a titolo esemplificativo e non esaustivo quelle inerenti la navigazione internet (art. 10), la partecipazione ai social media (art. 14) e le sanzioni (art.19)

3.4 - Modalità di lavoro in smart working: per le prestazioni lavorative eseguite con la modalità di lavoro denominata "Smart Working" si rimanda nello specifico all'art. 18 precisando che il contenuto del DUDI si intende vincolante anche per i lavoratori in Smart working ad eccezione delle disposizioni che confliggono con quanto stabilito al citato art. 18

4. Utilizzo del Personal Computer

4.1 - Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

4.2 - Il personal computer dato in affidamento all'utente permette l'accesso alla rete dei Titolari solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 5).

4.3 - I Titolari rendono noto che il personale incaricato che opera presso il servizio SIA è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dei Titolari, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio SIA ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

4.4 - Il personale incaricato del servizio SIA ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o a seguito di rilevazioni di problemi tecnici del sistema informatico/telematico. In quest'ultimo caso, e sempre che non si

ADOPERA PATRIMONIO E INVESTIMENTI CASALECCHIO DI RENO S.R.L. Via dei Mille 9, 40033 Casalecchio di Reno (Bo)
P.IVA C.F. 02780831208 Libro Verbali delle Decisioni dell'Amministratore Unico

APPREPA PATRIMONIO E INVESTIMENTI CASALECCHIO DI RENO S.R.L.
P.IVA C.F. 02780831208 Libro Verbali delle Decisioni dell'Amministratore Unico
Via dei Mille, 9 40033 Casalecchio di Reno (Bo)

pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione preventiva della necessità dell'intervento stesso.

4.5 - Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio SIA per conto dei Titolari, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno o scaricati dalla rete, sussistendo in tali casi il grave pericolo di introdurre virus informatici e/o di alterare funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione può esporre i Titolari a responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dei Titolari, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

4.6 - Salvo preventiva espressa autorizzazione del personale del servizio SIA, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

4.7 - Ogni utente deve prestare la massima attenzione ai supporti e periferiche di origine esterna (hard-disk, DVD, fotocamere, apparati multimediali, ecc ...), avvertendo immediatamente il personale del servizio SIA nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 11) relativo alle procedure di protezione antivirus.

4.8 - Ogni utente che dovrà, per qualsiasi motivo, lasciare incustodita temporaneamente la propria postazione di lavoro, sarà tenuto a bloccare l'accesso alla propria sessione tramite un sistema di blocco del sistema operativo che richieda l'inserimento della password di accesso per effettuare l'operazione di sblocco. I personal computer dotati di sistema operativo Windows appartenenti al sistema informatico dell'Unione prevedono un sistema di blocco automatico della sessione utente che si attiva autonomamente dopo 15 minuti di inattività. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

4.9 - Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. Tale modalità permette di evitare cospicui sprechi di energia elettrica ed ai software antivirus e altri software dediti alla sicurezza dei pc di poter effettuare aggiornamenti ed operazioni che richiedono un riavvio. Eventuali eccezioni vanno segnalate e concordate con il servizio SIA. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso (si faccia riferimento al punto 4.8).

5. Gestione delle password e degli account

5.1 - Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del servizio SIA, previa apertura di un ticket di assistenza (secondo le indicazioni di cui al punto 12) da parte del Dirigente/Responsabile del servizio indicante l'ambito nel quale verrà inserito ed andrà ad operare, il nuovo utente.

5.2 - Le singole credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal SIA, associato ad una parola chiave (password) riservata che dovrà venir **custodita dall'incaricato con la massima diligenza e non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del servizio SIA.

5.3 - Le credenziali di autenticazione si distinguono tra:

A. password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete (accesso al Personal Computer)
B. password per l'accesso ai singoli applicativi (software)

Il SIA è impegnato a far convergere in maniera automatica le password degli applicativi (punto B) con la stessa della rete (punto A) in modo da semplificare la gestione degli account da parte degli utenti e di uniformare le modalità di gestione delle stesse password (come previsto al successivo punto 5.4).

5.4 Le password devono sempre rispettare le seguenti condizioni:

- deve avere un lunghezza minima di 10 caratteri
- non deve contenere il nome dell'account dell'utente o parti del nome completo dell'utente che superano due caratteri consecutivi
- deve contenere almeno 3 caratteri delle 4 categorie:
  - una lettera maiuscola (dalla A alla Z)
  - una lettera minuscola (dalla a alla z)
  - un numero (da 0 a 9)
  - un carattere non alfanumerico (per esempio: !, $, #, %, _, & ecc.)

La password deve essere modificata al primo utilizzo e periodicamente ogni 90 giorni ai sensi della normativa in vigore, secondo la procedura di modifica proposta automaticamente all'utente. Non si potranno inoltre ri-utilizzare le precedenti 5 password.

La password, inoltre, non deve contenere riferimenti agevolmente riconducibili all'utente (es data di nascita, nome di familiari etc).

5.4 - Le password devono essere personali e segrete, e pertanto non devono essere comunicate o cedute a nessuno.

5.5 - Non è consentito effettuare l'accesso ad una qualunque dotazione informatica con le credenziali personali di accesso di un altro utente.

5.6 - Non è consentito l'uso di credenziali di accesso "generiche" non riconducibili ad una singola persona per effettuare l'accesso ad una qualunque dotazione informatica. Eventuali casi particolari andranno eventualmente concordati tra il Dirigente/Responsabile di servizio richiedente ed il servizio SIA.

5.7 In caso di cessazione del rapporto di lavoro, tutti gli account individuali dell'utente verranno immediatamente sospesi e, dopo dieci giorni lavorativi dalla data di cessazione, dismessi a meno di una richiesta effettuata tramite l'apertura di un ticket di assistenza (secondo le indicazioni di cui al punto 12) da parte del Dirigente/Responsabile di servizio. Le modalità di sospensione e cancellazione delle caselle di posta elettronica individuali vengono specificate nel punto 9.15.

6. Utilizzo delle periferiche, delle cartelle condivise e della rete informatica

6.1 - Per l'accesso alla rete dei Titolari ciascun utente deve utilizzare le proprie credenziali di autenticazione.

6.2 - Per cartella condivisa (unità di rete) si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.

6.3 - Le cartelle presenti nei server dei Titolari sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del servizio SIA. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno al PC - non sono soggetti a salvataggio da parte del personale incaricato del servizio SIA. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

6.4 - Risulta opportuno che ciascun utente, provveda alla pulizia periodica (almeno ogni tre mesi) di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.

6.5 - Il personale del SIA può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

6.6 - Nella gestione dei sistemi informatici aziendali, il SIA potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo

punto 15.2), per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 4.3), e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

6.7 - L'utente deve attenersi ad usare un metodo di archiviazione di file e cartelle consono, non creando un numero di livelli di sottocartelle superiore a 11 e utilizzando nomi di file e cartelle che non superano singolarmente i 20 caratteri, in modo che l'intero percorso del singolo file non superi i 260 caratteri. Il non rispetto del metodo soprastante può portare a comportamenti anomali sulle operazioni comuni che vengono effettuate su file e cartelle (apertura, rinomina, copia e incolla, taglia incolla, ripristino, ecc)

6.8 - Ogni Ente ed Azienda può disporre di alcune unità di rete condivise:

A. Unità **Servizi,** lettera **Q:**, contente le directory dei singoli servizi accessibili solamente al Dirigente/Responsabile di servizio e del relativo personale.
B. Unità **Tutti**, lettera **R:** Risulta essere uno spazio condiviso da tutti o parte degli utenti del singolo Ente/Azienda
C. Unità **Software**, lettera **P:** Risulta essere uno spazio condiviso gestito dal servizio SIA per l'uso di particolare software che non deve essere utilizzato come spazio di archiviazione.

6.9 - Ogni utente può disporre di una cartella di rete privata identificata con il proprio username e dalla lettera **U:** nella quale solo il singolo utente dispone dei diritti di accesso. Per tale ragione tale cartella non deve essere dedicata ad archiviare documenti di interesse dell'intero servizio. Per tale cartella privata valgono gli stessi principi dei punti 6.3 e 6.4.

6.10 - L'accesso alle unità di rete da parte degli utenti ed ogni successiva modifica, deve essere autorizzato dal Dirigente/Responsabile del servizio tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12, specificando le cartelle per le quali si richiede l'accesso.

7. Utilizzo di altri dispositivi elettronici

7.1 - Tutti i dispositivi elettronici dati in dotazione al personale dai Titolari devono considerarsi strumenti di lavoro: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni fissi, PC portatili, tablet, telefoni cellulari, smartphone, stampanti, scanner etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete dei Titolari o di condividere documenti, dati e materiali ivi conservati e/o trattati.

7.2 - Dispositivi elettronici personali: con riferimento all'uso di dispositivi elettronici personali (telefoni cellulari, smartphone, tablet, notebook, etc), quando lo richiedano esigenze connesse alla tipologia di lavoro, è consentito l'uso di dispositivi personali per finalità lavorative (es. controllo e gestione poste elettronica) nel rispetto delle seguenti prescrizioni:

- i dispositivi personali dovranno non essere liberamente accessibili ma bloccati con il più efficace tra i seguenti sistemi di protezione disponibile sul dispositivo utilizzato (in ordine di efficacia): PIN, impronta digitale, riconoscimento facciale;
- l'accesso alla posta elettronica non dovrà avvenire con password salvate direttamente sul dispositivo;
- non è consentito salvare file / allegati sui propri dispositivi (con particolare riferimento a documenti contenenti dati personali);
- si può controllare la posta elettronica solo se il dispositivo è ad uso esclusivamente personale e quindi non in condivisione con altre persone

7.3 - L'utente resta responsabile del singolo dispositivo assegnato che deve custodire con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del servizio SIA per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare il servizio SIA, e comunque al massimo entro 24 ore dal fatto.

7.4 - Con riferimento ai telefoni aziendali e telefoni cellulari/smartphone, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività

lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è consentito nei seguenti casi:

- assegnazione di telefono aziendale DUAL SIM
- assegnazione di telefono aziendale con singola SIM aziendale con ripartizione spese per chiamate personali
- assegnazione di SIM aziendale installata su telefono personale (DUAL SIM)

Nei casi di uso promiscuo sopra indicati, valgono le prescrizioni in materia di sicurezza indicate nel presente capitolo.

7.5 - Si precisa, peraltro, che le disposizioni previste nel presente documento ai punti 4), 8), 9), 10), 11) e 14) dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

7.6 Viene infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Dirigente/Responsabile di servizio.

7.7 - Il Dirigente/Responsabile di servizio si impegna ad eliminare, ove è possibile, le periferiche personali in favore di quelle di rete (periferiche condivise), che permettono un risparmio nei costi di gestione, limitando le periferiche personali esclusivamente ai casi in cui sia indispensabile per ragioni di servizio o di riservatezza (per periferica condivisa si intende stampante, scanner, plotter o qualsiasi altro dispositivo elettronico che può essere utilizzato in contemporanea da più uffici).

7.8 - Il Dirigente/Responsabile di servizio vigila sul corretto utilizzo dei device portatili e ne è corresponsabile assieme al lavoratore che deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

7.9 - I lavoratori a cui vengono dati in dotazione uno o più device portatili, devono abilitare, accettare ed effettuare nel minor tempo possibile gli aggiornamenti di sistema che il device propone e segnala.

7.10 - I device portatili non sono cedibili a terzi estranei all'Ente e devono essere utilizzati ai soli fini istituzionali.

7.11 - In caso di perdita o smarrimento di un device aziendale o personale - ma che sia comunque utilizzato per visualizzare dati aziendali (telefono o mail) la persona a cui è affidato o è titolare del dispositivo ha l'obbligo di presentare denuncia all'Autorità Giudiziaria e dare tempestiva comunicazione al SIA e al Comune che ha attribuito il device, per gli adempimenti conseguenti allo smarrimento.

7.12 - Si definiscono invece device portatili personali, qualunque device che non sia di proprietà di uno dei Titolari. Con riferimento ai device personali, non sono consentite:

- le connessioni a qualunque presa di rete delle presenti nelle reti cablate dei Titolari
- le connessioni al pc di di proprietà dei Titolari di qualunque device portatile personale

E' assolutamente vietato la connessione a prese di rete o pc di proprietà dei Titolari di qualunque dispositivo portatile di provenienza sconosciuta o di proprietà di cittadini.

In caso di eventi pubblici, presentazioni, talk in cui è necessario la trasmissione o proiezione video di materiale digitali/informatico (es: presentazioni Power Point) proveniente da relatori esterni ai Titolari, si richiede l'invio preventivo dello stesso materiale.

8. Utilizzo e conservazione dei supporti rimovibili

8.1 - Tutti i supporti rimovibili e/o magnetici (supporti USB, chiavette USB, floppy disk, CD e DVD riscrivibili, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

8.2 - L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

8.3 - E' vietato l'utilizzo di supporti rimovibili personali (es. chiavette USB). Per la condivisione o la visualizzazione di documenti fuori delle sedi di lavoro si consiglia fortemente l'uso di Google Drive facente parte della piattaforma G-suite in dotazione a tutto il personale. In casi di comprovata necessità, supporti rimovibili (non personali ma consegnati dall'Ente) potranno essere utilizzati. Resta fermo il divieto di utilizzare tali supporti per fini personali caricando file non attinenti l'attività lavorativa.

8.4 - Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio SIA e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possono venire salvati documenti, dati ed altro materiale, dovrà porsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del servizio SIA.

9. Gestione ed utilizzo della posta elettronica ed altri strumenti di condivisione documenti

9.1 - La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.2 - È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del servizio SIA. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

9.3 - La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti o non costituenti corrispondenza lavorativo/istituzionale e soprattutto allegati ingombranti. Si sottolinea infatti che la casella di posta elettronica è uno strumento di lavoro e non un archivio documentale.

9.4 - È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo. In caso di dubbi non si deve procedere all'apertura di allegati ma contattare il servizio SIA per chiarimenti.

9.5 - Ogni servizio può essere dotato di una casella di posta elettronica di servizio o di un gruppo di posta elettronica. Tale scelta viene concertata tra il Dirigente/Responsabile ed il servizio SIA valutando gli aspetti tecnici, organizzativi ed economici e poi formalizzata tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12.

9.6 - Una casella di posta elettronica di servizio risulta essere una casella di posta a tutti gli effetti cui si deve accedere tramite il sistema di "delega" gestito dal sistema di posta elettronica.

Un gruppo di posta elettronica di servizio, invece, risulta essere un indirizzo di posta elettronica che semplicemente consegna tutte le email ricevute dal gruppo alle caselle di posta individuali dei componenti del gruppo stesso.

9.7 - La creazione, la cancellazione e le relative autorizzazioni di accesso ad una casella di posta elettronica di servizio e/o l'appartenenza ad un gruppo di posta elettronica di servizio devono essere autorizzate dal Dirigente/Responsabile tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12).

9.8 - Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui i Titolari si fossero dotati, tale utente dovrà attenersi alle disposizioni previste nell'eventuale ulteriore apposito Regolamento aziendale a ciò dedicato e che va comunque a completare ed integrare il presente documento.

9.9 - Al fine di garantire la continuità dell'attività lavorativa, in caso di assenza programmata e prolungata (ad es. per ferie), gli utenti sono tenuti ad utilizzare l'apposita funzionalità di sistema "Risponditore automatico" che invia

automaticamente al mittente un messaggio di risposta, avvisando dell'assenza del destinatario del messaggio e relativo periodo e indicando eventuali modalità alternative per contattare la struttura.

9.10 - La gestione delle caselle di e-mail avviene in modo centralizzato sulla piattaforma cloud denominata "G-Suite" di Google. L'accesso a tali caselle avviene mediante l'utilizzo del browser di navigazione. Per tutto il pacchetto Google G-Suite (Google Gmail, Google Drive, Google Calendar, ecc) viene consigliato ed incoraggiato l'uso Google Chrome o, in alternativa, Mozilla Firefox.

9.11 - I titolari esortano tutti i Dirigenti, Responsabili, Amministratori e chiunque possa avere dati sensibili o altri dati da tutelare nella propria casella di posta elettronica ad aumentare la protezione del proprio account abilitando il sistema di "verifica in due passaggi" (o autenticazione a due fattori) che permette di aggiungere un ulteriore livello di sicurezza alla fase di accesso al proprio account. Per il supporto all'attivazione della verifica in due passaggi è possibile richiedere il supporto del SIA tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12.

9.12 - Non è consentita l'installazione e l'uso di client di posta elettronica nei personal computer (es. Microsoft Outlook, Mozilla Thunderbird), salvo che per specifiche esigenze concordate con il servizio SIA.

9.13 - La gestione delle caselle di e-mail nei device mobili smartphone e tablet, di servizio, deve avvenire tramite le app ufficiali Google (presenti negli store Google Play, Apple Store e/o negli store dei singoli produttori dei device) se compatibili con il device. In caso di non compatibilità, l'utente può richiedere, tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12), la consulenza del servizio SIA per individuare il client di posta migliore per il singolo device.

9.14- Ogni Ente afferente all'Unione può disporre di due gruppi di posta elettronica:

- **dipendenti@...** le email indirizzate a questo gruppo verranno ricevute solamente da tutti gli utenti che sono dipendenti di quel certo Ente
- **tutti@...** le email indirizzate a questo gruppo verranno ricevute da tutti gli utenti che hanno un indirizzo email con il dominio dell'ente (es: @comunexyz.bo.it). Nel caso di un Comune questo permetterà di raggiungere anche gli Amministratori che hanno la casella di posta elettronica istituzionale ed eventuali account di servizio

Entrambi vanno utilizzati **solo** per comunicazioni di servizio e/o istituzionali. I gruppi per invio massivo di email sono verificabili al link sottostante:
https://sites.google.com/unionerenolavinosamoggia.bo.it/ucrls-sia/documentazione/gruppi-liste-distribuzione

L'utilizzo di questi indirizzi deve sempre essere preventivamente comunicato/autorizzato dal proprio Responsabile di servizio.

In caso di invio agli indirizzi sopra indicati di comunicazioni istituzionali, è fatto divieto per i destinatari di utilizzare l'opzione "rispondi a tutti", rimanendo possibile per eventuali chiarimenti rispondere solo al mittente dell'email

9.15 In caso di **cessazione del rapporto di lavoro:**

A. la casella di posta individuale dell'utente verrà immediatamente sospesa il primo giorno della data di cessazione.
B. al decimo giorno lavorativo successivo alla data di sospensione (coincidente alla data di cessazione del rapporto di lavoro come al punto 9.15.A), a meno di una richiesta tramite l'apertura di un ticket di assistenza, (secondo le indicazioni di cui al punto 12) da parte del corrispettivo Dirigente/Responsabile di servizio, **verrà effettuato un backup della casella e la stessa verrà cancellata definitivamente.** Tale backup verrà eliminato definitivamente dopo esattamente 1 anno dalla data di effettuazione dello stesso.
C. almeno quindici giorni prima della sospensione dell'account (coincidente alla data di cessazione del rapporto di lavoro), l'utente della casella dovrà attivare una risposta automatica in cui dovrà indicare
   a. data di cessazione del rapporto di lavoro
   b. indirizzi email e contatti alternativi per le finalità di servizio
D. **non è consentito disporre (né richiedendo al servizio SIA né in autonomia) l'inoltro automatico dei messaggi delle casella di posta dell'utente cessante verso nessun'altra casella o gruppo di posta elettronica, in ottemperanza al provvedimento del Garante della Privacy 456 del 2015.**

9.16 - Si sottolinea che i punti sopra elencati del presente paragrafo 9 per la posta elettronica, vanno considerati vigenti anche per l'utilizzo dei servizi compresi nella stessa suite di prodotti G-Suite (es: Google Drive,

Google Calendar, Google Site, ecc) tramite i quali gli utenti possono condividere informazioni e documenti informatici inerenti la propria attività lavorativa.

E' espressamente vietato utilizzare gli strumenti di condivisione di Google Drive per pubblicare documenti direttamente sul web. In caso di necessità, prima di procedere, è obbligatorio ricevere l'autorizzazione da parte del proprio Dirigente/Responsabile.

10. Utilizzo e navigazione in Internet

10.1 - Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10.2 - In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica ad esempio) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del servizio SIA);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Dirigente/Responsabile di servizio e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

10.3 - Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolari rendono peraltro nota l'adozione della presenza di specifici sistemi di blocco e/o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una serie di "black list".

10.4 - Gli eventuali controlli, compiuti dal personale incaricato del servizio SIA ai sensi del precedente punto 4.3), potranno avvenire mediante sistemi di controllo dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre dodici mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dei Titolari.

10.5 - L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso in seguito ad una richiesta da parte del Dirigente/Responsabile di servizio al servizio SIA tramite l'apertura di un ticket di assistenza secondo le indicazioni di cui al punto 12).

L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti o autorizzati. A tale scopo vengono svolti controlli automatici che possono impedire l'accesso utilizzando dispositivi non abilitati.

11. Protezione antivirus

11.1 - Il sistema informatico dei Titolari è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

11.2 - Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere l'elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale del servizio SIA tramite telefonata ai tecnici o, in caso di mancata risposta, tramite l'apertura di un ticket di assistenza secondo le indicazioni del paragrafo 12.

11.3 - Ogni dispositivo rimovibile e/o magnetici di provenienza esterna ai Titolari dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio SIA.

12. Servizi e procedure di assistenza informatica

12.1 - Le procedure operative per le richieste di assistenza/servizi di cui al successivo punto 12.2) al servizio SIA, sono regolate da apposita procedura di apertura di ticket al portale web dedicato presente nella rete intranet dell'Unione:

https://pyunione.unionerenolavinosamoggia.bo.it/

Qualunque richiesta di assistenza informatica deve quindi essere segnalata tramite l'apertura di un ticket e **non sono modalità valide la telefonata, l'invio di una email o il raccolto de visu** a meno di casi particolari concordati con il Responsabile del servizio SIA. Sono caso particolari:

- servizi di sportello ai cittadini
- personale in servizio in sedi che non hanno l'accesso alla rete intranet dell'Unione

Poiché il portale di gestione delle richieste di assistenza è stato attivato in primo luogo a garanzia dei richiedenti che in tal modo possono monitorare lo stato dei propri ticket ed il periodo di giacenza degli stessi, oltre che per dotare i tecnici di un unico spazio in cui siano visibili e concentrate tutte le richieste aperte, **al di fuori dei casi particolari sopra indicati, una richiesta di assistenza informatica effettuata fuori del sistema di ticketing non verrà considerata né evasa dal personale tecnico del servizio SIA.**

Al fine di garantire una corretta e tempestiva assistenza, nel ticket si chiede di indicare necessariamente:

- un recapito telefonico diretto a cui essere contattati
- l'ubicazione della sede di lavoro (municipio, smart working etc)

12.2 - Il SIA tra le sue attività gestisce le principali richieste di assistenza/servizio, ovvero:

A. richiesta di acquisto, sostituzione di un personal computer, stampante, scanner e altre apparecchiature
B. richiesta di abilitazione all'accesso alla rete Internet
C. richiesta di abilitazione a specifici siti, servizi
D. richiesta di creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica e/o gruppi di servizio
E. richiesta di accesso alle informazioni presenti nelle cartelle condivise di servizio
F. richiesta di creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete comunale
G. richiesta di installazione di un nuovo applicativo
H. richiesta di abilitazione agli eventuali servizi erogati sulle Intranet per l'accesso a banche dati esterne (SIATEL, Servizi di Partout, e altri servizi on-line);
I. richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati interne (Anagrafe, Protocollo, ed altri servizi);
J. richiesta di ripristino del personal computer, stampante o altro dispositivo fornito dall'ente
K. richiesta di ripristino del funzionamento di software e programmi applicativi installati ed autorizzati
L. richiesta di dotare il personale di firma digitale (aperta dai responsabili di servizio) o di rinnovo della firma digitale

12.3 - Il personale tecnico del SIA effettua genericamente assistenza "da remoto" (senza recarsi in loco dall'utente) tramite software appositi di teleassistenza. La connessione ad un pc di un utente avviene sempre in accordo verbale con l'utente richiedente supporto e la procedura di connessione richiede, nel software di teleassistenza:

A. l'inserimento di una password da parte del tecnico del servizio SIA
B. l'approvazione esplicita da parte dell'utente

La presa in carico delle richieste di cui al punto 12.2) non è garantita qualora non venga rispettata la modalità descritto al punto 12.1). Salvo i casi indicati al punto 12.1), vengono considerate richieste "pendenti" solo quelle registrate tramite ticket nel portale della assistenze.

12.4 - Il personale tecnico del SIA non è autorizzato ad effettuare alcuna assistenza né consulenza per quanto riguarda personal computer e device mobili personali che non sono di proprietà del Titolari, salvo i casi di utilizzo di tali apparati dettato dalla necessità di lavorare in modalità smart working per i quali si rimanda all'art. 18.

13. Utilizzo delle stampanti e dei materiali di consumo

13.1 - L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi limitando le stampe ai soli casi in cui sia strettamente necessario per ragioni di lavoro. Ogni Dirigente/Responsabile di servizio è inviato a prendere contatti con il servizio SIA (per quanto di competenza) per lo studio di processi che siano finalizzati alla riduzione del consumo di carta.

14. Partecipazioni a social media

14.1 - L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, ecc, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dai Titolari attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 10.2).

14.2 - Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, i Titolari ritengono comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti degli stessi Titolari.

14.3 - La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dai Titolari riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners dei Titolari stesso. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dei Titolari; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi del Titolare, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale dei Titolari.

14.4 - L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Dirigente/Responsabile di servizio.

14.5 - L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso i Titolari, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.

14.6 - Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Dirigente/Responsabile di servizio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con i Titolari, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili ai Titolari.

15. Osservanza delle disposizioni in materia di Privacy

15.1 - È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, co[n] indicato nella lettera di designazione ad incaricato del trattamento dei dati/soggetto terzo.

15.2 - Gli strumenti tecnologici considerati nel presente documento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto qui indicato, anche conformemente al successivo paragrafo 16, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendo stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 17), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

15.3 - Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, il dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare procederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

16. Accesso ai dati trattati dall'utente

16.1 - Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del servizio SIA o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti punti 4.3) e 4.4), a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

17. Sistemi di controlli graduali

17.1 - In caso di anomalie, il personale incaricato del servizio SIA effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del servizio in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

17.2 - Per le finalità di cui al punto precedente, si comunica che i controlli ad oggi tecnologicamente pos[sibili] sono i seguenti:

a) controllo sui file di log prodotti da:
   - sistemi operativi
   - apparati di rete
   - software antivirus e sicurezza informatica
b) verifica attributi (tipologia, dimensioni etc) di file all'interno delle cartelle di rete e visualizzazione degli stessi

Da tali controlli è possibile reperire diverse informazioni sull'utilizzo da parte degli utenti delle dotazioni informatiche tra cui si evidenziano le principali:

- siti web visualizzati
- contenuti delle cartelle di rete
- stato di accensione dei pc anche fuori dell'orario di lavoro
- esecuzione di applicativi non consentiti

17.3 - In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

18. Modalità di Smart working

18.1 Per i casi in cui l'attività lavorativa venga prestata in modalità di smart working, la strumentazione utile al dipendente per lo svolgimento dell'attività lavorativa (pc, connessione, telefono, etc.) può essere anche di proprietà dello stesso (come indicato dalla Circolare n.1 del 2020 del dipartimento della funzione pubblica ed alla conseguente Sintesi circolare smart working).

18.2 - Per i casi in cui l'attività lavorativa venga prestata in modalità di smart working, oltre a richiamare tutte le disposizioni elencate all'interno del presente documento, ad eccezione di quelle incompatibili con il presente articolo, si conferma la necessità di rispettare i seguenti principi funzionali all'osservanza ed alla corretta applicazione del Reg. UE 2016/679 (GDPR):

1. in presenza di problematiche tecniche o di sicurezza informatica che impediscano o ritardino sensibilmente lo svolgimento dell'attività lavorativa in smart working, anche derivanti da rischi di perdita o divulgazione di informazioni dell'Ente, il dipendente sarà tenuto a dare tempestiva informazione al proprio responsabile (designato al trattamento).

2. fermo restando che la sede di lavoro resta invariata ad ogni effetto di legge e di contratto, in occasione della prestazione lavorativa effettuata in smart working, il dipendente potrà effettuare la prestazione in altro luogo purché presso strutture o spazi riservati, riparati e protetti, secondo le indicazioni date in base alle linee guida per la protezione dei dati e la sicurezza. Il lavoratore è tenuto alla più assoluta riservatezza sui dati personali e sulle informazioni dell'Ente in suo possesso e/o disponibili sul sistema informatico dell'Ente che dovrà custodire con la massima cura, ed è altresì tenuto ad adottare tutte le precauzioni necessarie a garantire la salvaguardia e lo svolgimento delle attività in condizioni di sicurezza.

3. non è consigliabile portarsi della documentazione cartacea presso le proprie abitazioni, laddove ciò sia indispensabile, previa autorizzazione del designato o del titolare del trattamento (anche tramite email), potranno essere portati solamente le copie, non gli originali, dei documenti non contenenti dati particolari (sensibili) o documenti d'identità o informazioni strettamente personali e che rivelino situazioni di disagio.

4. il lavoratore è comunque tenuto a custodire con diligenza la documentazione, i dati e le informazioni dell'Ente utilizzati in connessione con la prestazione lavorativa, nonché al rispetto delle previsioni del Regolamento UE 679/2016 e del D.lgs. 196/2003 – così come novellato dal D.lgs 101/18 - in materia di privacy e protezione dei dati personali.

5. i dispositivi forniti dall'Ente non dovranno essere modificati nelle loro impostazioni di misure di sicurezza e di funzionamento.

6. laddove siano utilizzati dispositivi personali, devono essere osservate le presenti prescrizioni:

   a. dispositivi protetti da password;
   b. dispositivi protetti da antivirus;

7. laddove il dispositivo personale sia un pc (desktop o notebook), tale pc dovrà rispettare i requisiti tecnici indicati nel documento tecnico "Accesso Citrix e Smart Working", già condiviso con i dipendenti e in costante aggiornamento in relazione all'evoluzione tecnologica.

8. laddove il dispositivo personale sia un pc (desktop o notebook), il cui uso sia promiscuo (condiviso con più persone) è bene:

   a. non salvare mai in locale documenti;
   b. [illegible]
   c. non salvare informazioni di log in;
   d. [illegible]

19. Sanzioni

19.1 - È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente documento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

ADOPERA PATRIMONI GESTIONI IMMOBILIARI CASALECCHIO DI RENO S.R.L. Via dei Mille, 9 40033 Casalecchio di Reno (Bo)
P.IVA C.F. 02780831208 Libro verbali delle Decisioni dell'Amministratore Unico

Determinazione dell'Amministratore Unico n. 03 del 02/02/2021

OGGETTO: PROCEDURA FINALIZZATA ALLA SOTTOSCRIZIONE DI UN CONTRATTO DI SERVIZIO PER AFFIDAMENTO INCARICO ESCLUSIVO DI VENDITA BENI MOBILI E ATTREZZATURE – APPROVAZIONE AVVISO ESPLORATIVO PER MANIFESTAZIONE DI INTERESSE.

L'AMMINISTRATORE UNICO

Premesso che:

- nel corso dell'anno 2020 è stata fatta una ricognizione dei beni e delle attrezzature presenti presso la sede operativa della Società in Via G. Rossa, 1 a Casalecchio di Reno;

- che a seguito di tale attività sono stati individuati beni e attrezzature non utilizzati e/o non più idonei all'uso ma suscettibili di alienazione e/o valorizzazione, ai sensi dell'art. 58 del d.l. n. 112/2008 convertito con modificazioni nella l. n. 133/2008;

- che parte di questi beni sono di proprietà del Socio Comune di Casalecchio di Reno al quale afferiva l'attività manutentiva prima del subentro di Adopera;

- la Giunta del Comune di Casalecchio di Reno nella seduta del 2 febbraio u.s. ha fornito parere favorevole alla procedura esplorativa riservandosi di adottare proprio atto di liberatoria e aggiornamento inventario al momento in cui verrà redatto elenco dei beni da parte dell'operatore aggiudicatario del servizio;

Dato atto che il D.Lgs n. 50/2016 e s.m.i. stabilisce:

- all'art. 95 stabilisce che prima dell'avvio delle procedure di affidamenti dei contratti pubblici (di lavori, servizi e forniture di beni) le amministrazioni aggiudicatrici, e quindi per analogia anche le società patrimoniali che fungono da stazioni appaltanti, determinano di contrarre in conformità alla propria organizzazione e/o regolamento;

- all'art. 30, comma 1, stabilisce che l'affidamento e l'esecuzione di appalti di opere, lavori, servizi, forniture e concessioni garantisce la qualità delle prestazioni e si svolge nel rispetto dei principi di economicità, efficacia, tempestività e correttezza. Nell'affidamento degli appalti e delle concessioni, le stazioni appaltanti rispettano, altresì, i principi di libera concorrenza, non discriminazione, trasparenza, proporzionalità, nonché di pubblicità con le modalità indicate nel presente codice…;

Considerato quanto disposto al comma 2 dell'art. 40 del D.Lgs 50/2016 e s.m.i. e quindi che a decorrere dal 18/10/2018 tutte le stazioni appaltanti devono utilizzare mezzi di comunicazione elettronica nell'ambito delle procedure di gara allo scopo di garantire l'integrità dei dati e la riservatezza delle offerte e delle domande di partecipazione.

Preso atto che:

- ✓ si intende sondare il mercato mediante la pubblicazione di un avviso di manifestazione d'interesse allo scopo di individuare gli operatori economici da invitare alla successiva fase di gara;
- ✓ espletare poi una procedura negoziata ai sensi dell'art. 1 del D.L. 76/2020 convertito in L. 120/2020 per l'affidamento di un incarico esclusivo di vendita beni mobili e attrezzature di Adopera s.r.l. o del Socio Comune di Casalecchio di Reno;

- ✓ il valore complessivo dell'incarico non è quantificabile in quanto dipenderà dal valore di vendita dei beni e delle attrezzature il cui elenco sarà stilato a carico dell'operatore economico che si aggiudicherà la procedura;

Redatti l'avviso di manifestazione d'interesse e l'istanza di partecipazione, che fanno parte integrante e sostanziale del presente provvedimento anche se non materialmente allegati, ma conservati agli atti d'ufficio;

Ritenuto di procedere alla pubblicazione per quindici giorni consecutivi dell'Avviso di Manifestazione d'Interesse sul sito ufficiale della Società e sulla home page del sito del Socio Comune di Casalecchio di Reno ritenendo assolto, con tali pubblicazioni, il dovere di pubblicità della procedura;

Considerato che occorre provvedere in questa sede all'approvazione dell'avviso di manifestazione d'interesse e l'allegata istanza di partecipazione;

Ritenuto opportuno individuare il Responsabile del Procedimento nell'Ing. Francesco M. Cellini nella sua qualità di Direttore Tecnico - Coordinatore;

Ravvisata la propria competenza all'adozione della presente determinazione ai sensi del mandato ricevuto e di quanto disposto dall'art. 20 dello Statuto societario.

Visti:

- il D. Lgs. 50/2016;
- l'art. 58 del d.l. n. 112/2008 convertito in l. n. 133/2008;

DETERMINA

per le ragioni di cui in premessa e che si intendono qui integralmente riportate e richiamate

- **di approvare** in questa sede l'Avviso di Manifestazione d'Interesse e l'allegata istanza di partecipazione, che restano conservati agli atti, per individuare gli Operatori Economici da invitare alla procedura negoziata per l'affidamento dell'incarico esclusivo di vendita beni mobili e attrezzature di Adopera s.r.l. o del Socio Comune di Casalecchio di Reno;

- **di procedere** alla pubblicazione per quindici giorni consecutivi dell'Avviso di Manifestazione d'Interesse sul sito ufficiale della Società e su quello del Socio Comune di Casalecchio di Reno assolvendo agli oneri di pubblicità previsti dalla normativa vigente;

- **di dare atto:**
  - che viene individuato quale responsabile del procedimento ai sensi dell'art. 3 della legge n. 241/1990 l'Ing. Francesco M. Cellini nella sua qualità di Direttore Tecnico - Coordinatore;
  - che il presente provvedimento ha validità dal momento della sua sottoscrizione;

- **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del D.Lgs 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del D.Lgs 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

141

Determinazione dell'Amministratore Unico n. 4 del 12/02/2021

OGGETTO: GESTIONE DEL SISTEMA DI TUTELA DEL DIPENDENTE CHE SEGNALA ILLECITI "WHISTLEBLOWING" AGGIORNAMENTO LINEE GUIDA

L'AMMINISTRATORE UNICO

Premesso che:

- il "**whistleblowing**" è la segnalazione compiuta da un lavoratore che, nello svolgimento delle proprie mansioni, si accorge di una frode, un rischio o una situazione di pericolo che possa arrecare danno all'azienda/ente per cui lavora, nonché a clienti, colleghi, cittadini, e qualunque altra categoria di soggetti.

- il "whistleblowing" è uno strumento legale atto a segnalare tempestivamente ad una serie di soggetti (Autorità Giudiziaria, Corte dei conti, Autorità Nazionale Anticorruzione, Responsabile anticorruzione all'interno del proprio Ente/Azienda): pericoli sul luogo di lavoro, frodi all'interno, ai danni o ad opera dell'organizzazione, danni ambientali, false comunicazioni sociali, negligenze mediche, illecite operazioni finanziarie, minacce alla salute, casi di corruzione o concussione e molti altri ancora.

Richiamate:

• la 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";

• le linee guida ANAC di cui alla determinazione n. 6/2015 inerenti la tutela del dipendente pubblico che segnala illeciti;

• il regolamento ANAC per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54 bis d.lgs n. 165/2001;

• la Delibera ANAC n. 690 del 1^ luglio 2020 che ha modificato l'intera struttura del precedente per consentire ad ANAC di esercitare il potere sanzionatorio in modo più efficace e celere e per svolgere un ruolo attivi nell'opera di emersione di fatti illeciti commessi nelle amministrazioni pubbliche;

• l'art. 54 del D.Lgs 165/2001 ed in particolare i commi 1, 3, 6, 7, 8 e 9;

Dato atto che:

- le Società sottoposte a controllo pubblico, dotate di un proprio modello organizzativo ex d.lgs 231/2001, che necessitano di ricevere anche le segnalazioni relative ai reati presupposto indicati nel decreto, devono essere dotate di un sistema conforme alle prescrizioni di sicurezza a tutela di segnalanti e segnalazioni previste dalla normativa vigente;

- la Società ha attivato una piattaforma software in modalità "Software as a service" di DigitalPA S.r.l., per la segnalazione degli illeciti alla quale è possibile accedere utilizzando l'indirizzo URL: https://adoperasrl.segnalazioni.net;

- la piattaforma utilizza un protocollo di crittografia che garantisce il trasferimento dei dati riservati, attraverso il codice univo ottenuto a seguito della segnalazione è consentito di dialogare con il

Responsabile della Prevenzione della Corruzione e della trasparenza in modo anonimo e spersonalizzato;

- il 23/10/2019 il Parlamento europeo ed il Consiglio hanno adottato la Direttiva 2019/1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione". Questa direttiva stabilisce norme minime comuni volte a garantire la protezione dei cd. whistleblowers negli ordinamenti dei Paesi Membri, e costituirà il riferimento normativo per i Paesi dove non sussiste alcuna regolamentazione nonché implementazione delle tutele per i Paesi, come l'Italia, dove il fenomeno era già stato oggetto di una normazione.

Visto il documento di aggiornamento del sistema di segnalazione: "Linee Procedurali per la segnalazione di illeciti o irregolarità e disciplina della tutela del dipendente che segnala illeciti", predisposto dal Responsabile della Prevenzione della Corruzione e Trasparenza nel febbraio 2021, che si allega al presente atto quale parte integrante.

Visti inoltre:
- la Legge 30 novembre 2017, n. 179
- il Regolamento ANAC 1.7.2020 e le linee guida;
- la L. 190/2012;
- il D.Lgs. 165/2001;

DETERMINA

per le motivazioni espresse in premessa:

- di confermare tutte le attività relative la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito del proprio rapporto di lavoro;

- di approvare il documento di aggiornamento del sistema di segnalazione: *"Linee Procedurali per la segnalazione di illeciti o irregolarità e disciplina della tutela del dipendente che segnala illeciti"*, predisposto dal Responsabile della Prevenzione della Corruzione e Trasparenza nel febbraio 2021, allegato al presente atto quale parte integrante;

- di dare incarico al Responsabile Prevenzione della Corruzione e Trasparenza di inserire nella formazione rivolta al personale le informazioni utili alla conoscenza del sistema di segnalazione;

- di dare atto:

- che il responsabile del procedimento ai sensi dell'art. 3 della legge n. 241/1990 è il firmatario del presente atto;
- che il presente provvedimento ha validità dal momento della sua sottoscrizione;

- di dare attuazione agli adempimenti di pubblicità prescritti dall'art. 29 del D.Lgs 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del D.Lgs 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

adopera
Patrimonio e investimenti Casalecchio di Reno S.r.l

LINEE PROCEDURALI PER LA SEGNALAZIONE DI ILLECITI O IRREGOLARITA' E DISCIPLINA DELLA TUTELA DEL DIPENDENTE CHE SEGNALA ILLECITI

aggiornamento febbraio 2021

Procedura aggiornata alla Legge 30 novembre 2017 n. 179

Sommario

1 PREMESSA 2
2 TITOLO I - PROCEDURE PER LA SEGNALAZIONE 4
2.1.1 Art. 1) Soggetti e contenuti del sistema di segnalazione 4
2.1.2 Art. 2) Procedure per la segnalazione 4
2.1.3 Art. 3) Attività di accertamento della segnalazione 5
3 TITOLO II - PRECAUZIONI PER LA TUTELA DEL SEGNALANTE 7
3.1.1 Art. 4) La tutela del segnalante 7
3.1.2 Art. 5) Segnalazione di discriminazioni 8
3.1.3 Art. 6) La responsabilità del segnalante 8
4 DISPOSIZIONI GENERALI 9
5 Appendice: allegato 1) Manuale utenti 10

1 PREMESSA

Adopera s.r.l., in considerazione della modifica apportata dalla legge 190/2012 (cd. legge anticorruzione) al D. Lgs. n. 165/2001 con l'inserimento dell'articolo 54 bis "*Tutela del dipendente pubblico che segnala illeciti*", così come modificato dall'art. 1 della Legge 30 novembre 2017 n. 179, su proposta del Responsabile della prevenzione della corruzione e della trasparenza, definisce e adotta la presente disciplina al fine di favorire la presentazione di segnalazioni di "*illeciti*" da parte dei propri dipendenti.

La normativa sopra richiamata ha introdotto nel nostro ordinamento una misura finalizzata a favorire la segnalazione da parte del dipendente, agli organi legittimati ad intervenire, di violazioni o irregolarità commesse ai danni dell'interesse pubblico. Una misura volta a fare emergere fattispecie di illeciti; già nota nei paesi anglosassoni come "*whistleblowing*".

Va detto, per quanto attiene alle segnalazioni, che si connotano come manifestazioni di senso civico attraverso cui il dipendente contribuisce all'emersione e alla prevenzione di rischi e di situazioni pregiudizievoli per la Società di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Dunque l'attività del segnalante non deve essere considerata in senso negativo assimilabile ad un comportamento delatorio, ma come fattore destinato a eliminare possibili forme di *"cattiva amministrazione"* e di "corruzione" all'interno della Società nel rispetto dei principi di legalità, di imparzialità e di buon andamento della Società sanciti dalla Costituzione all'articolo 97.

Si rammenta che il decreto legge n. 90 del 2014, convertito con modificazione dalla legge n. 114 del 2014, preveda la possibilità per il dipendente di presentare segnalazioni di illeciti **direttamente** all'Autorità nazionale Anticorruzione (A.N.A.C.).

In ottemperanza alle disposizioni sopra richiamate il Responsabile della prevenzione della corruzione e della trasparenza della Società, adotta le presenti Linee guida per la segnalazione da parte **dei dipendenti e collaboratori della Società** di illeciti o di irregolarità, al fine di rimuovere fattori che possono ostacolare o disincentivare il ricorso a detto istituto, eliminare timori di ritorsioni discriminazioni, chiarire eventuali dubbi ed incertezze e tutelare i dipendenti, secondo quanto stabilito nel Piano triennale di prevenzione della corruzione aggiornamento al triennio 2020-2022 (P.T.P.C.) e quanto richiamato nel Modello Organizzativo Gestionale "MOG" adottato con determina dell'Amministratore Unico n. 4 del 28.01.2019 e modificato, integrato ed aggiornato con successive determinazioni n. 10 del 25.06.2019 e n. 2 del 28.01.2020.

L'obiettivo perseguito dalla presente procedura è quello di fornire ai dipendenti/collaboratori della Società indicazioni operative circa l'oggetto, i contenuti, i destinatari e le modalità di trasmissione delle segnalazioni, anche alla luce dei recenti orientamenti forniti dall'Autorità Nazionale Anticorruzione relativamente a:

a) destinatari della segnalazione;

b) oggetto e i contenuti della segnalazione;

c) modalità di trasmissione delle segnalazioni;

d) *forme di tutela dei dipendenti e dei collaboratori.*

Preme, infine, precisare come per **"illecito" e "corruzione"** debba intendersi ogni forma di condotta "attiva o passiva" che contrasti con le normative legislative, statutarie, regolamentari ma anche con le prassi e le misure organizzative della Società.

Infatti come precisa la Circolare n. 1 del Dipartimento della Funzione Pubblica del 25.01.2013, la legge n. 190/2012" non contiene una definizione della "corruzione", che viene quindi data per presupposta:

"In questo contesto, il concetto di corruzione deve essere inteso in senso lato, come comprensivo delle varie situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati. Le situazioni rilevanti sono quindi evidentemente più ampie della fattispecie penalistica, che, come noto, è disciplinata negli artt. 318, 319 e 319-ter, c.p., e sono tali da comprendere non solo l'intera gamma dei delitti contro la pubblica amministrazione disciplinati nel Titolo II, Capo I, del codice penale, ma anche le situazioni in cui a prescindere dalla rilevanza penale venga in evidenza un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite".

Conseguentemente non esiste una lista tassativa di illeciti o irregolarità che possono costituire l'oggetto della segnalazione, ma sono rilevanti quelle inerenti comportamenti, rischi, reati o irregolarità a danno dell'interesse pubblico.

ADOPERA PATRIMONIO E INVESTIMENTI CASALECCHIO DI RENO S.R.L. Via dei Mille, 9 40033 Casalecchio di Reno (Bo)
P.IVA C.F. 02780831208 Libro Verbali delle Decisioni dell'Amministratore Unico

144

2 TITOLO I - PROCEDURE PER LA SEGNALAZIONE

2.1.1 ART. 1) SOGGETTI E CONTENUTI DEL SISTEMA DI SEGNALAZIONE

Adopera s.r.l. individua nel Responsabile della Prevenzione della Corruzione e della trasparenza, il soggetto destinatario delle segnalazioni da parte del dipendente o collaboratore che intende denunciare un illecito o un'irregolarità all'interno della Società, di cui è venuto a conoscenza, nell'esercizio dell'attività lavorativa e che può riguardare comportamenti, rischi, reati o irregolarità a danno dell'interesse pubblico.

Ribadito che non è possibile redigere una lista completa e tassativa di fattispecie di comportamenti, reati o irregolarità, a titolo meramente esemplificativo, si può precisare che la segnalazione può riguardare azioni o omissioni:

a) che potrebbero configurare reati (es.: peculato, corruzione, concussione, abuso d'ufficio, malversazione a danno dello Stato, rifiuto o omissione d'atti d'ufficio, falso ideologico, falso materiale, turbata libertà degli incanti, frode nelle pubbliche forniture, truffa, furto, minaccia, violenza privata);

b) che costituiscono violazioni al Codice di comportamento;

c) che consistono in illegittimità o illeciti amministrativi e che possono comportare danni patrimoniali alla Società o ad altra pubblica amministrazione o alla collettività.

Il "segnalante", pertanto, non deve utilizzare l'istituto in argomento per scopi meramente personali o per effettuare rivendicazioni di lavoro contro superiori gerarchici o la Società, per le quali occorre riferirsi ad specifiche discipline.

2.1.2 ART. 2) PROCEDURE PER LA SEGNALAZIONE

Adopera ha attivato una piattaforma software per la segnalazione degli illeciti.

È possibile accedere alla piattaforma utilizzando l'indirizzo URL: https://adoperasrl.segnalazioni.net. La piattaforma utilizza un protocollo di crittografia che garantisce il trasferimento dei dati riservati, attraverso il codice univo ottenuto a seguito della segnalazione è consentito di dialogare con il Responsabile della Prevenzione della Corruzione e della trasparenza in modo anonimo e spersonalizzato.

Il sistema ha inviato o invierà ai nuovi dipendenti/collaboratori una comunicazione via mail con le credenziali di accesso temporanee (Username e Password). Accedendo alla piattaforma si ha a disposizione anche il manuale d'uso.

Le credenziali dovranno essere custodite gelosamente e non divulgate.

Il dipendente accede al servizio per la segnalazione di illeciti attraverso browser e da qualsiasi dispositivo (pc, smartphone, tablet) con le credenziali (username e password) che ciascun segnalatore può acquisire registrandosi autonomamente nella piattaforma.

Ciascun dipendente riceverà tramite mail l'indirizzo a cui accedere per effettuare la segnalazione; ai dipendenti/collaboratori neo assunti verrà fornita indicazione di detto indirizzo. Le modalità per accedere sono riportate nel Manuale utenti, allegato in forma sintetica al presente atto e reperibile sul sito di Adopera. Detto manuale in forma aggiornata è altresì reperibile, dopo la registrazione, nell'Area riservata della piattaforma (link in alto a destra).

Il servizio prevede l'indicazione di tutti gli elementi utili a consentire di procedere alle dovute ed appropriate verifiche e controlli a riscontro della fondatezza dei fatti che sono ricompresi nell'oggetto della segnalazione.

Si deve rappresentare l'indispensabilità che la denuncia presentata dal "segnalante" sia: 4 – circostanziata – riguardi fatti riscontrabili e conosciuti direttamente dal denunciante e non riportati o riferiti da altri soggetti – contenga una chiara descrizione dei fatti, tempi e modi con cui si è realizzata la presunta condotta illecita.

2.1.3 ART. 3) ATTIVITÀ DI ACCERTAMENTO DELLE SEGNALAZIONI

Il Responsabile della Prevenzione della Corruzione e della trasparenza, all'atto del ricevimento della segnalazione, provvede ad avviare la procedura interna per la verifica dei fatti rappresentati nella dichiarazione del segnalante, investendo le strutture interne.

Il Responsabile della Prevenzione della Corruzione e della trasparenza, nel rispetto della massima riservatezza e dei principi di imparzialità, potrà effettuare ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti (indicati dal segnalante) che possono riferire sugli episodi segnalati.

Il Responsabile della Prevenzione della Corruzione e della trasparenza potrà contattare direttamente il "segnalante" e riceverlo in un luogo protetto, anche al di fuori dei locali della Società, per garantire la sua massima riservatezza, per acquisire ogni ulteriore tipo di informazione utile circa l'episodio che denuncia. La segnalazione, dopo avere subito l'oscuramento in corrispondenza dei dati identificativi del segnalante, potrà essere trasmessa, a cura del "Responsabile", ad altri soggetti interessati per consentire loro le valutazioni del caso e/o le eventuali iniziative in merito da intraprendere: le risultanze dell'istruttoria dovranno essere comunicate al "Responsabile" non oltre 30 giorni dalla ricezione della segnalazione, salvo proroga, per giustificato motivo, di ulteriore 15 giorni.

Qualora, all'esito delle opportune verifiche la segnalazione risulti fondata, in tutto o in parte, il "Responsabile", in relazione alla natura della violazione, provvederà:

1. a comunicare l'esito dell'accertamento al Responsabile del Servizio di appartenenza dell'autore della violazione accertata, affinché provveda all'adozione dei provvedimenti di competenza, incluso, sussistendone i presupposti, l'esercizio dell'azione disciplinare.

2. ad adottare o a proporre di adottare, se la competenza è di altri soggetti o organi, tutti i necessari provvedimenti amministrativi per il pieno ripristino della legalità.

Resta impregiudicato e autonomo dalla procedura in discorso, l'obbligo di presentare denuncia all'Autorità Giudiziaria competente relativamente alle fattispecie penalmente rilevanti.

Il Responsabile della Prevenzione della Corruzione, a conclusione degli accertamenti, informa dell'esito o dello stato degli stessi il segnalante, secondo la modalità dallo stesso prescelta e con le opportune precauzioni a garanzia della sua tutela, se necessario.

3 TITOLO II - PRECAUZIONI PER LA TUTELA DEL SEGNALANTE

3.1.1 ART. 4) LA TUTELA DEL SEGNALANTE.

L'identità del segnalante deve essere protetta in ogni contesto, a partire dal momento dell'invio della segnalazione. Pertanto non può essere rivelata senza il suo espresso consenso e coloro che ricevono o sono coinvolti nella gestione della segnalazione, anche solo accidentalmente, sono tenuti a tutelare la riservatezza di tale informazione.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

L'identità del segnalante può essere rivelata solo nel caso in cui:

1. vi sia il consenso da parte del medesimo;

2. la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. (Si tratta dei casi in cui la segnalazione è solo uno degli elementi che hanno fatto emergere l'illecito, ma la contestazione avviene sulla base di altri fatti da soli sufficienti a far scattare l'apertura del procedimento disciplinare nei confronti del denunciato);

3. la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità sia assolutamente indispensabile per la difesa dell'incolpato. Questa circostanza può emergere solo a seguito dell'audizione dell'incolpato ovvero dalle memorie difensive che lo stesso produce nel procedimento.

La segnalazione, come previsto dall'art. 54 bis, comma 4, del d.lgs. n. 165 del 2001 s.m.i., è sottratta all'accesso, disciplinato dagli artt. 22 e seguenti della legge 241/1990 e s.m.i.

Colui che, ai sensi dell'art. 54 bis del d.lgs. n. 165 del 2001, quale superiore gerarchico, riceve informazioni da un dipendente, di un illecito o di una irregolarità, è tenuto a proteggerne l'identità e a invitarlo a effettuare segnalazione anche al Responsabile della Prevenzione della Corruzione oppure a provvedere direttamente, secondo una delle modalità di cui all'art. 2.

In caso di omissione e di mancata protezione del segnalante, il dirigente risponde disciplinarmente e, se sussistono i presupposti, incorre nelle altre forme di responsabilità previste dall'ordinamento.

La comunicazione al Responsabile della Prevenzione della Corruzione non integra gli estremi della violazione dell'obbligo di protezione, da parte del dirigente, dell'identità del segnalante.

3.1.2 ART. 5) SEGNALAZIONE DI DISCRIMINAZIONI

I segnalanti che denunciano all'Autorità Giudiziaria o alla Corte dei Conti o all'Autorità Nazionale Anticorruzione (A.N.AC) o al superiore gerarchico o al Responsabile della Prevenzione della Corruzione, condotte illecite di cui siano venuti a conoscenza in ragione del rapporto di lavoro, non possono essere sanzionati, licenziati o sottoposti ad alcuna misura discriminatoria per motivi collegati, direttamente o indirettamente, alla denuncia.

Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione.

Il segnalante che ritiene di aver subito una discriminazione deve dare notizia circostanziata dell'avvenuta discriminazione al Responsabile della Prevenzione della Corruzione medesimo, per metterlo in condizioni di valutarne la fondatezza e i possibili interventi di azione, per ripristinare la situazione o per rimediare agli effetti negativi della discriminazione in via amministrativa e per perseguire, disciplinarmente, l'autore della discriminazione.

L'adozione di misure discriminatorie a seguito di segnalazione che abbia avuto anche come destinatario il Responsabile della Prevenzione della Corruzione, può essere altresì segnalata direttamente, ai sensi e per gli effetti del comma 3, art. 54 bis, d.lgs. n. 165/2001 s.m.i., al Dipartimento della Funzione Pubblica, per i provvedimenti di competenza, dallo stesso interessato o per il tramite delle organizzazioni sindacali maggiormente rappresentative nella Società;

La Società promuove, a tutela dei segnalanti, un'efficace attività di sensibilizzazione, comunicazione e formazione sui diritti e gli obblighi relativi alla segnalazione degli illeciti, a tutela del pubblico interesse, nell'ambito dei percorsi di formazione sull'etica pubblica è il codice di comportamento dei pubblici dipendenti.

3.1.3 ART. 6) LA RESPONSABILITÀ DEL SEGNALANTE

La tutela del segnalante non può essere assicurata nei casi in cui questi incorra, con la denuncia, in responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale, o in responsabilità civile extracontrattuale, ai sensi dell'art. 2043 del codice civile. Inoltre, l'anonimato del segnalante non può essere garantito in tutte le ipotesi in cui l'anonimato stesso non è opponibile per legge (come per esempio nel corso di indagini giudiziarie, tributarie, ispezioni di organi di controllo). Nel caso in cui, a seguito di verifiche interne, la segnalazione risulti priva di ogni fondamento saranno valutate azioni di responsabilità disciplinare o penale nei confronti del segnalante, salvo che questi non produca ulteriori elementi a supporto della propria denuncia.

4 DISPOSIZIONI GENERALI

Le violazioni degli obblighi previsti dal presente atto configurano altre responsabilità disciplinare, per inosservanza a disposizioni di servizio, se, a seconda della fattispecie, non sono individuabili illeciti disciplinari più gravi. La procedura individuata presente atto per il *whistleblowing*, nonché i profili di tutela del segnalante saranno sottoposti a revisione periodica per verificare possibili lacune o incomprensioni anche da parte dei dipendenti e collaboratori.

5 Appendice: allegato 1) Manuale utenti

ULTERIORI DOC. DEPOSITATI AGLI ATTI 12/02/2021

Determinazione dell'Amministratore Unico n. 05 del 22/03/2021

OGGETTO: APPROVAZIONE "RELAZIONE DEL RPCT ANNO 2020" E ADOZIONE DELLA PROPOSTA DI "AGGIORNAMENTO DEL PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE PER IL TRIENNIO 2021-2023".

L'AMMINISTRATORE UNICO

Richiamate in merito le seguenti disposizioni normative:

- art. 1 comma 8 della L. 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica Amministrazione" che dispone che si adotti ogni anno il Piano triennale di prevenzione della corruzione, contenente l'analisi e la valutazione dei rischi specifici di corruzione e gli interventi organizzativi volti a prevenirli;

- D.Lgs 33/2013 avente ad oggetto "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";

- D.Lgs 39/2013 avente ad oggetto "Disposizioni in materia di inconferibilità ed incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'art. 1, commi 49 e 50, della L. 190/2012";

- art. 19 del D.L. 90/2014 che trasferisce ad ANAC le competenze in materia di prevenzione della corruzione e di promozione della trasparenza nelle Pubbliche Amministrazioni, attribuendo alla stessa il compito di adottare il PNA Piano Nazionale Anticorruzione quale atto di indirizzo rivolto a tutte le Amministrazioni che devono adottare i PTPCT, nonché il potere di vigilanza sulla qualità dei Piani adottati dagli Enti;

- D.Lgs 97/2016 avente ad oggetto: "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del D.Lgs 33/2013, ai sensi dell'art. 7 della L. 124/2015, in materia di riorganizzazione delle amministrazioni pubbliche".

Richiamati i seguenti atti assunti dall'Autorità Nazionale Anticorruzione – ANAC:

- Delibera n. 831/2016 "approvazione del PNA 2016";

- Delibera n. 1309/2016 "Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, co. 2, del D.Lgs 33/2013"

- Determina n. 1310/2016 approvazione "Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel D.Lgs 33/2013 così come modificato dal D.Lgs 97/2016";

- Determina n. 1134/2017, in vigore dal 5/12/2017, avente ad oggetto: "Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e dagli enti di diritto privato controllati e partecipati dalle pubbliche economici";

- Determina n. 1208//2017 avente ad oggetto: "Approvazione definitiva dell'Aggiornamento 2017 al Piano Nazionale Anticorruzione";

- Delibera n. 141/2018 avente ad oggetto "Attestazioni OIV, o strutture con funzioni analoghe, sull'assolvimento degli obblighi di pubblicazione al 31 marzo 2018 e attività di vigilanza dell'Autorità;

- Delibera 1064 del 13.11.2019 di approvazione del PNA 2019 con i relativi allegati:

1. Indicazione rischi corruttivi;
2. Rotazione del personale;
3. Riferimenti normativi sul ruolo e sulle funzioni del RPCT.

Richiamate inoltre le proprie precedenti determinazioni:
- n. 3 del 18/04/2017;
- n. 1 del 10/01/2018;
- n. 5 del 28.01.2019;
- n. 10 del 25.6.2019,
con la quali si è provveduto agli adempimenti in materia di PTPC per il periodo 2016-2019.

Esaminate:
- la relazione al PTPC anno 2020;
- la proposta di aggiornamento del PTPC 2021-2023;
predisposte dalla Responsabile della Prevenzione della Corruzione, della Trasparenza e dell'accesso civico, nominata con propria determinazione n. 5 del 10/04/2018.

Considerato che:

- sono stati costantemente aggiornati i dati collegati al Programma di Trasparenza e al Piano di prevenzione della corruzione previsti dalla L. 190/2012 e dal D.Lgs 33/2013 e loro s.m.i.

- ogni elemento utile alla correttezza e trasparenza è meritevole di attenzione e contribuisce positivamente all'immagine della Società soprattutto in considerazione della tutela degli interessi degli stakeholders aziendali siano essi individui, istituzioni e utenti in genere;

- la corretta attuazione della normativa è da considerarsi la continuazione delle politiche aziendali che hanno portato all'introduzione del Codice di Comportamento (Regolamento interno);

- il PTPCT è strettamente connesso al Modello Organizzativo ex D.Lgs 231/2001 "MOG" che costituisce il sistema strutturato ed organico di procedure e regole che la Società utilizza e rispetta allo scopo di ridurre il rischio di commissione dei reati con l'obiettivo di costituire l'esimente ai fini della responsabilità amministrativa degli enti.

Dato atto che non si è provveduto ad apportare variazioni al MOG in vigenza in quanto rispondente anche alle variazioni normative intervenute mentre si è proceduto ocn l'aggiornamento del Piano Triennale della Trasparenza e Anticorruzione 2021-2023 predisposto dalla RTPC e da considerarsi sempre atto integrativo del MOG.

Vista la proposta di aggiornamento del Piano della Trasparenza e gestione degli adempimenti in relazione agli obblighi della trasparenza di cui al D.Lgs 33/2013 e s.m.i, ritenuta accoglibile.

Dato atto infine che:

- tutte le attività svolte da Adopera sono strumentali a quelle dei propri Comuni Soci;
- è comunque opportuno che la Società adotti atti e provvedimenti autonomi e/o distinti da quelli dei propri Soci.

Considerato in ultimo che MOG e PTPCT devono rimanere raccordati e complementari.

Acquisiti i pareri dell'Organo di Vigilanza Avv. Alessandro Vasi e della Responsabile della Prevenzione della Corruzione, della Trasparenza e dell'accesso civico Sig.ra Grazia Fantini.

Ravvisata la propria competenza all'adozione della presente determinazione ai sensi del mandato ricevuto e di quanto disposto dall'art. 20 dello Statuto societario.

Visto il Comunicato del Presidente dell'Autorità del 2 dicembre 2020 che, tenuto conto dell'emergenza sanitaria determinata dal Codid-19 differisce al 31 marzo 2021 i termini per la redazione della relazione al Piano 2020 e l'aggiornamento dello stesso per il periodo 21-23.

Visti:
- il D.Lgs 267/2000;
- D.Lgs 231/2001 e s.m.i.;
- D.Lgs 81/2008 e s.m.i.;
- la Determinazione ANAC n. 1134/2017;
- le Delibere ANAC n. 141/2018, n. 1064/2019 e n. 213/2020;

DETERMINA

per le motivazioni ampiamente espresse in premessa, che si intendono qui interamente richiamate:

- **di confermare** il Modello Organizzativo ex D.Lgs 231/2001 "MOG" di Adopera S.r.l. così come vigente e pubblicato;

- **di ribadire** che le attività svolte per la realizzazione di misure organizzative di prevenzione e controllo di carattere generale, secondo quanto disposto all'art. 1, comma 9 della L. 190/2012, previste nei Piani esistenti, sono regolari;

- **di prendere atto** della relazione dell'RPCT anno 2020, depositata agli atti d'ufficio;

- **di adottare** l'aggiornamento del Piano triennale della Prevenzione della corruzione e della Trasparenza triennio 2021-2023 (PTPCT) predisposto dal RPCT, contenuto nella relazione al PTPCT 2020, depositato agli atti d'ufficio;

- **di mantenere attivo** il dialogo con i Comuni Soci a favore di una fattiva regia delle attività poste in essere dalla Società con particolare riferimento al ruolo di direzione, coordinamento e controllo analogo dell'azione ai sensi di legge;

- **di informare** l'Organo di Vigilanza Avv. Alessandro Vasi ed i Comuni Soci di quanto approvato ed adottato e trasmettere copia completa di tutta la documentazione allo stesso OdV ed ai rispettivi Responsabili della Trasparenza;

- di dare ampia informazione dei documenti aggiornati ai dipendenti della Società;

- di dare attuazione agli adempimenti di pubblicità prescritti dall'art. 29 del D.Lgs. 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del D.Lgs. 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

Determinazione dell'Amministratore Unico n. 6 del 26/03/2020

OGGETTO: LIQUIDAZIONE "COMPENSI PER PRODUTTIVITÀ ANNO 2020" AI DIPENDENTI DELLA SOCIETÀ – RICONOSCIMENTO ACCONTO.

L'AMMINISTRATORE UNICO

Richiamati:

- la deliberazione del Consiglio Comunale n. 26 del 25/03/2021 con la quale è stato approvato il Piano Operativo Aziendale della Società per l'anno 2021;

- lo Statuto Societario approvato nel suo ultimo aggiornamento quale allegato A) dell'atto Notaio Paolo Tavalazzi Rep. n. 13516/6919 del 17/01/2019;

- il Sistema di misurazione e valutazione delle performance individuale del 19/06/2014 e l'accordo relativo all'Attribuzione dell'incentivo monetario sulla base della performance, sottoscritto dalla delegazione trattante in data 19/05/2016;

- l'Accordo Unico, siglato dal sindacato e dai rappresentanti sindacali, del 19/05/2016 ai punti 12 e l'integrazione dell'11/02/2015 con la quale viene previsto un importo minimo da erogare con il cedolino di marzo e quindi nel mese di aprile.

Verificato che:

- la spesa per i compensi incentivanti per l'anno 2020, unitamente alle altre spese di personale, non supera i limiti disposti dalla normativa vigente (L. 122/2010 e 114/2014);

- le somme sono utilizzate nel rispetto delle destinazioni di cui all'accordo stipulato.

Ritenuto opportuno procedere per il personale dipendente alla liquidazione in acconto dei compensi di produttività per l'anno 2020, per una somma complessiva di € 23.598,91 comprensiva di oneri e IRAP, come di seguito dettagliata:

Cognome Nome	*Acconto PREMIO*	*TOTALE COSTO ACCONTO*
Antonicelli Nicola	€ 479,45	€ 661,05
Brandani Claudio	€ 363,01	€ 486,94
Brionesi Valentina	€ 0,00	€ 0,00
Cellini Francesco Maria	€ 493,15	€ 663,17
Ciobanu Catalin Gheorghe	€ 457,53	€ 632,14
Dalla Bona Alessandro	€ 493,15	€ 675,95
Destrieri Simone	€ 500,00	€ 665,61
Domicoli Luigi	€ 42,47	€ 59,78
Falanga Pasquale	€ 500,00	€ 665,61
Fantini Grazia	€ 500,00	€ 670,69
Ferrara Marcello	€ 491,78	€ 678,47
Froio Massimo	€ 463,01	€ 639,71
Gallozza Silvana	€ 491,78	€ 659,66

Gamberini Fabrizio	€ 495,89		€ 666,85
Gasperini Giovanni	€ 354,08		€ 502,35
Gherardi Roberto	€ 493,15		€ 693,36
Grandi Fabrizio	€ 493,15		€ 699,65
Graziani Gian Luca	€ 390,41		€ 530,32
Guidetti Federica	€ 498,63		€ 650,35
Laffi Daniele	€ 19,18		€ 25,08
Marchetti Roberto	€ 447,95		€ 617,99
Mauceri Salvatore	€ 495,89		€ 666,85
Nadalini Davide	€ 497,26		€ 699,98
Ognibene Fausto	€ 369,32		€ 482,94
Palmas Giorgio Umberto	€ 500,00		€ 665,61
Parazza Monica	€ 394,74		€ 514,84
Parrino Benedetto	€ 457,53		€ 649,12
Poggi Emanuele	€ 390,40		€ 538,60
Prince Sara	€ 126,03		€ 164,37
Resca Roberto	€ 500,00		€ 684,16
Sacanna Stefano	€ 475,34		€ 638,16
Samiolo Simone	€ 500,00		€ 671,26
Sassi Paolo	€ 500,00		€ 709,37
Soddu Sandro	€ 500,00		€ 665,61
Spalazzese Franco	€ 500,00		€ 653,83
Testigrosso Serena	€ 446,58		€ 582,46
Ungureanu Florin	€ 453,42		€ 626,47
Vaccari Stefano	€ 375,56		€ 528,66
Venturi Fausto	€ 500,00		€ 690,82
Zanetti Carlo	€ 249,32		€ 335,27
	€ 16.699,16	€	22.713,10
IRAP	3,90%	€	885,81
	TOTALE	€	23.598,91

Accertato che:

- il premio 2020 è stato accantonato e rilevato come costo nel Bilancio definitivo al 31.12.2020;

- le somme destinate all'acconto sui compensi incentivanti per l'anno 2020 non superano i limiti disposti dalla normativa vigente (L. 122/2010 e 114/2014) e vengono utilizzate nel rispetto delle destinazioni di cui agli accordi stipulati.

Verifica la competenza dell'Amministratore Unico ad assumere il presente atto.

Visti:

- il d.lgs 267/2000;
- il d.lgs 165/2001;
- lo Statuto della Società;
- il Sistema di misurazione e valutazione delle performance individuale del 19/06/2014;

- l'accordo per l'attribuzione dell'incentivo monetario sulla base della performance del 19/05/2016 e la sua successiva integrazione;
- i poteri assegnati all'Amministratore Unico dall'art. 20 dello Statuto e del Provvedimento di individuazione a firma del Sindaco del Comune di Casalecchio di Reno in data 23/04/2019 - Prot. n. 13588;

DETERMINA

per quanto espresso in premessa, che si intende integralmente richiamato:

- **di provvedere** alla liquidazione ai dipendenti dell'acconto dei compensi di produttività per l'anno 2020 per una somma complessiva di € 23.598,91 comprensiva di oneri e IRAP;

- **di dare atto che**:

- il premio 2020 è stato accantonato e rilevato come costo nel Bilancio definitivo al 31.12.2020;

- la spesa per tali compensi non supera i limiti disposti dalla normativa vigente (L. 122/2010 e 114/2014) e che la stessa viene utilizzata nel rispetto delle destinazioni di cui all'accordo stipulato;

- il Responsabile del Procedimento ha provveduto ad accertare preventivamente la compatibilità della spesa con le disponibilità del POA 2021;

- il saldo dei compensi incentivanti viene rinviato ad apposito atto da assumersi nel mese di luglio 2020 e che tale atto terrà conto dell'acconto riconosciuto con la presente determinazione;

- **di dare mandato** al Servizio Personale affinché predisponga quanto necessario per la liquidazione delle somme suindicate;

- **di dare atto:**
- che il responsabile del procedimento ai sensi dell'art. 3 della legge n. 241/1990 è il firmatario del presente atto;
- che il presente provvedimento ha validità dal momento della sua sottoscrizione;

- **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del d.lgs 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del d.lgs 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

Dott. Marco Castellani
Amministratore Unico

Determinazione dell'Amministratore Unico n. 07 del 08/06/2021

OGGETTO: AFFIDAMENTO INCARICO DI ORGANISMO DI VIGILANZA "ODV" PER BIENNIO 2021-2023 ALL'AVV. ALESSANDRO VASI DI RAVENNA IN CONTINUITA' CON IL SERVIZIO PRESTATO.

L'AMMINISTRATORE UNICO

Richiamate le seguenti disposizioni normative:

- Decreto Legislativo 8 giugno 2001, n. 231 e s.m.i.;

- "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01" approvate da Confindustria il 7 marzo 2002 e successivamente aggiornate al 21 luglio 2014;

- Decreto Legislativo n. 81/2008 e s.m.i.

Premesso che:

- si è optato per la scelta di un organo monocratico cui affidare il potere di accedere alla documentazione aziendale rilevante, raccogliere le informazioni idonee a monitorare situazioni dell'attività aziendale e sollevare Adopera S.r.l. dal rischio di illeciti;

- con propria determina n. 2 del 31/01/2018, a seguito di pubblica selezione, è stato nominato Organismo di Vigilanza "OdV" di Adopera S.r.l. l'Avvocato Alessandro Vasi con studio a Ravenna in Via Fiorita, 45 – P.IVA 02123960391;

- che l'insediamento dell'OdV è avvenuto in data 23 maggio 2018 con redazione di apposito verbale, depositato agli atti d'ufficio.

Dato atto che ad oggi l'OdV ha provveduto ad espletare con regolarità le seguenti attività:

- monitoraggio delle procedure di controllo interno ed attivazione di eventuali procedure aggiuntive se ritenute carenti;
- ricognizioni dell'attività aziendale per mappare gli ambiti a rischio;
- verifiche periodiche mirate su operazioni o atti posti in essere negli ambiti a rischio, così come definiti dal Modello;
- promozione di iniziative per la diffusione della conoscenza e della comprensione del "Modello";
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del "Modello";
- coordinamento con le altre funzioni aziendali per monitorare le attività degli ambiti a rischio;
- controllo dell'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nel "Modello";
- indagini volte all'accertamento di eventuali violazioni delle prescrizioni del "Modello";
- segnalazione delle criticità relative all'esistenza di eventuali flussi finanziari atipici e predisposizione di opportune soluzioni operative.

Visto che:

- con propria determina n. 4 del 28/01/2019 Adopera ha adottato il Modello 231 MOG elaborato in collaborazione con l'OdV;
- nel corso dell'ultimo triennio, in particolare a seguito delle sempre più numerose pronunce della giurisprudenza e delle normative inerenti l'anticorruzione e trasparenza dell'azione amministrativa, è risultato evidente che il "Modello 231" ha costituito uno strumento indispensabile ad Adopera quale società che gestisce servizi pubblici.

Richiamata la propria determina n. 5 del 22/03/2021 con la quale di conferma il MOG e si prende atto dell'aggiornamento del Piano della Trasparenza e Anticorruzione 2021-2023, redatto dal RPCT.

Acquisito il parere della Responsabile Trasparenza e Anticorruzione Sig.ra Grazia Fantini.

Ritenuto opportuno:

- confermare la necessità per la società Adopera di essere affiancata dall'Odv;
- affidare in via diretta, ai sensi dell'art. 1, comma 2, lett. a) L. 120/2020, l'incarico per l'ulteriore periodo 2021-2023, in continuità con le attività svolte, all'Avv. Alessandro Vasi;
- confermare la congruità della somma riconosciuta annualmente per l'incarico di OdV in € 5.000,00 oltre oneri ed I.V.A. di legge in considerazione della complessità dell'incarico da espletare.

Ravvisata la propria competenza all'adozione del presente atto.

Visti:

- il d.lgs n. 267/2000;
- il d.lgs n. 231/2001 e s.m.i.;
- il d.lgs n. 81/2008 e s.m.i.;
- le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01" approvate da Confindustria il 7/3/2002 ed aggiornate al 21/7/2014;

DETERMINA

per le motivazioni ampiamente espresse in premessa:

- di approvare la proposta inerente le attività di OdV Avv. Alessandro Vasi confermata in data 07/06/2021 e con le stesse condizioni economiche preesistenti;

- di affidare in via diretta, ai sensi dell'art. 1, comma 2, lett. a) L. 120/2020, l'incarico di Organismo di Vigilanza, "OdV", di Adopera S.r.l. per il periodo maggio 2021-aprile 2023 all'Avv. Alessandro Vasi con studio in Via Fiorita, 45 a Ravenna – P.IVA 02123960391;

- di quantificare in € 5.000,00 (cinquemila euro) oltre oneri ed IVA nelle misure di legge il compenso annuo da riconoscere all'Avv. Alessandro Vasi, prevedendo tale spesa all'interno dei POA dei rispettivi anni di competenza;

- **confermare** le attività sinora svolte dall'Avv. Vasi ed in continuità con le stesse conferirgli mandato a monitorare, verificare, promuovere tutte le attività che riterrà opportune e necessarie quale OdV nonché segnalare e rimuovere le criticità legate agli ambiti a rischio di corruzione;

- **promuovere** il costante aggiornamento documentale delle attività di OdV che verranno svolte allo scopo di assicurare un corretto flusso formativo e informativo;

- **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del d.lgs. n. 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del d.lgs. n. 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

Determinazione dell'Amministratore Unico n. 08 del 25/06/2021

OGGETTO: APPROVAZIONE "CODICE DI COMPORTAMENTO".

L'AMMINISTRATORE UNICO

Richiamati:

- il D.P.R. 16 aprile 2013, n. 62 recante "*Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*";

- l'Intesa del 24 luglio 2013 tra Governo, Regioni e Enti Locali per l'attuazione dell'art. 1, cc. 60 e 61, L. 6 novembre 2012, n. 190 recante: "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*";

- l'art. 54, c. 5, D.Lgs. n. 165/2001;

- la deliberazione n. 75/2013 dell'Autorità Nazionale Anticorruzione ad oggetto: "*Linee guida in materia di codici di comportamento delle pubbliche amministrazioni (art. 54, comma 5, d.lgs. n. 165/2001)*".

Considerato che l'adozione del codice di comportamento con caratteristiche confacenti al nuovo assetto organizzativo della Società permetterà di avere uno strumento di rilievo nell'ambito del complesso delle iniziative per la prevenzione della corruzione.

Valutata la necessità di avere un documento che ripropone i principi dettati dal codice nazionale di comportamento di cui al citato D.P.R. n. 62/2013, con una minima personalizzazione rispetto alle esigenze della Società;

Vista la proposta presentata dal Gruppo di Lavoro costituito per la formulazione del documento;

Dato atto che:

- con nota del 24/03/2021 l'Avv. Alessandro Vasi ha espresso, in qualità di OdV, parere favorevole alla proposta di documento e agli adempimenti conseguenti;

- con nota prot. n. 626 del 26/05/2021 tramite PEC il Responsabile per la prevenzione della corruzione ha inviato ai Comuni Soci e alle Organizzazione Sindacali informativa relativa all'adozione del Codice di comportamento, richiedendone il parere in ordine all'applicabilità;

- la bozza del Codice è stata affissa in bacheca al piano terreno della sede societaria, caricata sul portale Zucchetti a servizio di tutti i dipendenti della Società e pubblicata sul sito della Società;

Visto che nei termini previsti non è pervenuta alcuna osservazione;

Esaurita la fase di consultazione lo schema di Codice è stato sottoposto all'RPCT che ha espresso parere favorevole come da nota interna Prot. n. 919 del 15/06/2021, depositata agli atti;

Visto infine lo Statuto Societario;

Determinata la propria competenza ad assumere il presente atto;

DETERMINA

1) **di approvare** l'allegato documento "Codice di comportamento", quale parte integrante del presente provvedimento;

2) **di dare atto che**:

- l'entrata in vigore di nuove leggi di rango superiore, generali e speciali, in materia di rapporti di lavoro e impiego, abrogano le norme del Codice, qualora risultino incompatibili;

- il Codice di comportamento verrà pubblicato sul sito internet della Società, nonché trasmesso tramite il portale Zucchetti a tutti i dipendenti e verrà allegato ai contratti di consulenza o di collaborazione a qualsiasi titolo, anche professionale;

- copia del Codice verrà consegnata ai titolari di organi e di incarichi negli uffici di diretta collaborazione dei vertici della Società, nonché ai collaboratori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore di Adopera;

- contestualmente alla sottoscrizione del contratto di lavoro o, in mancanza, all'atto di conferimento dell'incarico, il Codice verrà consegnato ai nuovi assunti;

3) **di dare inoltre atto che:**

- sull'applicazione del Codice sono chiamati a vigilare i Direttori Tecnici, l'RPC, l'Organismo di Vigilanza e l'Ufficio Personale che si occupa dei procedimenti disciplinari;

- i Direttori Tecnici, con il supporto dell'Ufficio Personale, attivano interventi finalizzati alla piena conoscenza e corretta applicazione del Codice;

4) **di dare atto, infine,** che il Codice entra in vigore dalla data di esecutività della presente deliberazione di approvazione e pertanto da tale data si ritiene abrogata tutta la normativa vigente incompatibile con le nuove disposizioni;

5) **di dare attuazione** agli adempimenti di pubblicità prescritti dall'art. 29 del d.lgs. n. 50/2016 e agli adempimenti inerenti la pubblicazione sul sito della Società nella sezione "Amministrazione Trasparente" nel rispetto dell'articolo 37 del d.lgs. n. 33/2013 e dell'art. 1, co. 32 della Legge 190/2012.

L'Amministratore Unico
Dott. Marco Castellani

adopera
Patrimonio e Investimenti Casalecchio di Reno S.r.l.

CODICE DI COMPORTAMENTO

adopera
Patrimonio e Investimenti Casalecchio di Reno S.r.l.

STUDIO CESARE NOTAIO IN MALALBERGO

Art. 1. Disposizioni di carattere generale

1. Il presente codice di comportamento, di seguito denominato "codice", definisce, ai sensi dell'articolo 54, comma 5, del decreto legislativo 31 marzo 2001, n. 165 [1], i doveri di diligenza, lealtà, imparzialità e servizio che vincolano alla cura dell'interesse pubblico, che il personale, incluso quello con qualifica dirigenziale [2], è tenuto a osservare.
2. Le disposizioni del presente codice specificano e integrano le previsioni contenute nel Codice di comportamento dei dipendenti delle pubbliche amministrazioni approvato con decreto del Presidente della Repubblica 16 aprile 2013, n. 62, che costituisce la base minima di ciascun codice di comportamento adottato dalle varie amministrazioni e le cui disposizioni devono ritenersi integralmente richiamate.

Art. 2. Ambito di applicazione

1. Gli obblighi di condotta previsti dal codice generale e dal presente codice sono applicabili a tutti i dipendenti di Adopera srl con qualsiasi tipologia di contratto.
2. Gli obblighi vengono estesi ai collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, nonché nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore di Adopera srl, per quanto compatibili.
   A tal fine, nei provvedimenti di incarico e nei contratti di collaborazione, consulenza e servizi, sono inserite apposite clausole di risoluzione o decadenza dal rapporto in caso di violazione degli obblighi in essi specificamente indicati, in quanto giudicati compatibili, fatta salva la possibilità, per Adopera srl, di stabilire obblighi ulteriori individuati sulla base del tipo di collaborazione prestata.
3. In caso di violazione di taluno degli obblighi di cui al secondo periodo del secondo comma del presente articolo, il Direttore tecnico competente provvede alla contestazione al collaboratore/appaltatore, assegnando un termine di 30 giorni per presentare le giustificazioni. Decorso infruttuosamente tale termine, oppure nel caso in cui le giustificazioni non siano ritenute idonee a escludere la violazione, se quest'ultima sia considerata grave, o comunque incompatibile con la prosecuzione del rapporto, ne dispone la risoluzione con provvedimento.

Art. 3. Obbligo di cortesia

1. Il personale dimostra massima cortesia e disponibilità nei rapporti con tutti gli utenti, i colleghi, i collaboratori, i fornitori e qualsiasi altro interlocutore, evitando qualsiasi discriminazione.

Art. 4. Regali compensi e altre utilità

1. I soggetti di cui all'art. 2 comma 1, evitano di ricevere benefici di ogni genere, non sollecitano né accettano, per sé o per altri, alcun dono o altra utilità, anche sotto forma di sconto, da parte di terzi, in relazione al ruolo ricoperto. Al di fuori di tale ipotesi è consentito ricevere "regali d'uso" purché di modico valore che, singoli o sommati ad altri pervenuti dal medesimo soggetto nella medesima occasione, cosiddetti regali plurimi, non superino il valore di € 150 nell'anno.
2. Nel caso in cui i soggetti di cui all'art. 2, comma 1, ricevano da terzi, in relazione al ruolo ricoperto, regali, benefici o altre utilità che, singoli o plurimi, non possano considerarsi "d'uso" e di modico valore ai sensi del comma 1, devono darne tempestiva comunicazione al Responsabile della Prevenzione della Corruzione.
3. I regali, nei casi previsti dal comma 2, sono comunque restituiti o acquisiti dalla Società che li destina ad iniziative di beneficenza.

Art. 5. Incarichi di collaborazione

1. Il divieto, di cui all'articolo 4, comma 6 del codice generale [3], ricomprende gli incarichi a titolo gratuito ed è posto anche rispetto a soggetti privati senza scopo di lucro.

[1] Art. 54, comma 5:"Ciascuna pubblica amministrazione definisce [...] un proprio codice di comportamento che integra e specifica il codice di comportamento di cui al comma 1".

2 ai fini del presente Codice di comportamento e in considerazione dell'Organigramma della Società si intendono "Dirigenti" i Direttori tecnici in quanto equiparati ai Funzionari responsabili di posizione organizzativa negli enti privi di dirigenza di cui all'Art. 13 comma 1 DPR 16 aprile 2013 n. 62

adopera
Patrimonio e Investimenti Casalecchio di Reno S.r.l.

2. I soggetti privati che abbiano o abbiano avuto un interesse economico significativo in decisioni o attività inerenti all'ufficio di appartenenza del dipendente sono, ad esempio, i soggetti controparte dell'azienda in azioni legali, gli aggiudicatari di appalti e sovvenzioni, i destinatari di autorizzazioni e i destinatari di attività di controllo o ispettiva.

Art. 6. Partecipazione ad associazioni od organizzazioni

1. Il dipendente che aderisca ad associazioni od organizzazioni i cui ambiti di interessi potrebbero interferire con lo svolgimento dell'attività dell'ufficio, entro 30 giorni da tale adesione ne dà comunicazione al Direttore Tecnico di riferimento, eventualmente utilizzando un protocollo riservato. Tali ambiti riguardano, in particolare, la partecipazione ad associazioni od organizzazioni il cui scopo sia omologo, simile o in potenziale contrasto con l'attività svolta dai settori di appartenenza dei singoli dipendenti.
2. Il Direttore tecnico che riceve la comunicazione di cui all'articolo 5, comma 1 del codice generale [4], ha l'obbligo di assicurare la riservatezza nel trattamento dei dati.
3. A seguito dell'esame delle segnalazioni, i Direttori tecnici valutano l'opportunità di assegnare i collaboratori ad altro incarico, al fine di evitare possibili situazioni di conflitto di interessi.

Art. 7. Comunicazione degli interessi finanziari

1. Il personale adempie alla disposizione di cui all'articolo 6, comma 1 [5], del codice generale, mediante comunicazione per iscritto effettuata immediatamente dopo l'assegnazione e indirizzata ai responsabili degli uffici. Questi ultimi hanno l'obbligo di assicurare la riservatezza nel trattamento dei dati e operano verifiche per accertare la completezza e la correttezza delle comunicazioni. I Direttori tecnici, con l'eventuale coinvolgimento del Responsabile della prevenzione della corruzione e della trasparenza (d'ora in avanti, RPCT), adottano, se necessario, le misure utili a rimuovere il conflitto, qualora quest'ultimo assuma un carattere strutturale.
2. Il personale segnala tempestivamente le variazioni intervenute rispetto agli interessi finanziari già comunicati.
3. Il Direttore tecnico che riceve la comunicazione ha l'obbligo di assicurare la riservatezza nel trattamento dei dati.
4. Le valutazioni inerenti le comunicazioni di cui al presente articolo, qualora effettuate nei confronti dei responsabili degli uffici, competono al RPCT; quelle nei confronti di quest'ultimo sono sottoposte all'Amministratore Unico.

Art. 8. Conflitto d'interessi e astensione

1. Il personale, qualora ricorrano i presupposti di cui all'articolo 7 [6] del codice generale, fatta eccezione per quelli disciplinati dal secondo comma del presente articolo, Il comunica tempestivamente al Direttore tecnico di riferimento e si astiene dal partecipare all'adozione di decisioni o attività. Il Direttore tecnico, verificata la situazione di conflitto d'interessi, sostituisce l'interessato.
2. Il dipendente, qualora ritenga che rispetto ad attività di propria competenza vi sia il coinvolgimento di persone con le quali abbia rapporti di frequentazione abituale, o grave inimicizia, oppure esistano altre gravi ragioni di convenienza per astenersi, prima di compiere qualsiasi atto rende tempestivamente al Direttore Tecnico di

[3] Art. 4, comma 6: *"Il dipendente non accetta incarichi di collaborazione da soggetti privati che abbiano, o abbiano avuto nel biennio precedente, un interesse economico significativo in decisioni o attività inerenti all'ufficio di appartenenza"*

[4] Art. 5, comma 1: *"Nel rispetto della disciplina vigente del diritto di associazione, il dipendente comunica tempestivamente al responsabile dell'ufficio di appartenenza la propria adesione o appartenenza ad associazioni od organizzazioni, a prescindere dal loro carattere riservato o meno, i cui ambiti di interessi possano interferire con lo svolgimento dell'attività dell'ufficio. Il presente comma non si applica all'adesione a partiti politici o a sindacati"*

[5] Art. 6, comma 1: *"Fermi restando gli obblighi di trasparenza previsti da leggi o regolamenti, il dipendente, all'atto dell'assegnazione all'ufficio, informa per iscritto il responsabile dell'ufficio di tutti i rapporti, diretti o indiretti, di collaborazione con soggetti privati in qualunque modo retribuiti che lo stesso abbia o abbia avuto negli ultimi tre anni, precisando:*
a) se in prima persona, o suoi parenti o affini entro il secondo grado, il coniuge o il convivente abbiano ancora rapporti finanziari con il soggetto con cui ha avuto i predetti rapporti di collaborazione;
b) se tali rapporti siano intercorsi o intercorrono con soggetti che abbiano interessi in attività o decisioni inerenti all'ufficio, limitatamente alle pratiche a lui affidate"

[6] Art. 7: *"Il dipendente si astiene dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri, ovvero di suoi parenti, affini entro il secondo grado, del coniuge o di conviventi, oppure di persone con le quali abbia rapporti di frequentazione abituale, ovvero, di soggetti od organizzazioni con cui egli o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito significativi, ovvero di soggetti od organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di enti, associazioni anche non riconosciute, comitati, società o stabilimenti di cui sia amministratore o gerente o dirigente. Il dipendente si astiene in ogni altro caso in cui esistano gravi ragioni di convenienza. Sull'astensione decide il responsabile dell'ufficio di appartenenza"*

adopera
Patrimonio e Investimenti Casalecchio di Reno S.r.l.

riferimento una comunicazione in forma scritta contenente ogni informazione utile a valutare la rilevanza del presunto conflitto. Se sia un soggetto apicale a ritenere di poter essere in conflitto, la comunicazione è inviata al RPCT. Il Direttore tecnico, dopo aver eventualmente chiesto chiarimenti al dipendente utili a valutare la situazione, si pronuncia per iscritto sulla rilevanza del conflitto, dandone comunicazione all'interessato. Se lo ritiene rilevante, individua per la trattazione della pratica un altro operatore.
3. Se necessario, le segnalazioni di cui ai commi 1 e 2 sono effettuate utilizzando un protocollo riservato.
4. Sono oggetto di comunicazione, ai sensi del comma 2, le situazioni che, pur non in grado di minare l'imparzialità del personale, sono tali comunque da poter essere percepite come una minaccia alla stessa.
5. Sono oggetto di comunicazione, ai sensi del comma 2, le situazioni di conflitto di interessi che emergano in riferimento ad attività vincolata, anche se rispetto a esse non si rileva un obbligo di astensione.
6. Se il conflitto di interessi è meramente apparente, quindi relativo a una situazione tale da non interferire con l'imparzialità del dipendente, quest'ultimo non ha l'obbligo di comunicarlo al Direttore tecnico; tuttavia, deve adoperarsi per far emergere, quando possibile, la situazione reale.
7. Qualora il dipendente sia effettivamente l'unico ad avere competenze sufficienti a trattare la pratica rispetto alla quale è emerso il conflitto di interessi, il Direttore tecnico (o, nel caso sia quest'ultimo in situazione di conflitto, il RPCT) avoca a sé la decisione, che viene assunta a seguito di istruttoria compiuta dall'operatore in situazione di conflitto.
8. I componenti le commissioni di selezione pubblica del personale rendono una dichiarazione con la quale attestano di non trovarsi nelle situazioni di conflitto d'interessi di cui all'articolo 7 del codice generale.

Art. 9. Prevenzione della corruzione

1. I Direttori tecnici verificano che siano attuate dal personale le misure necessarie alla prevenzione degli illeciti nella società. In particolare, essi rispettano e fanno rispettare le prescrizioni contenute nel piano triennale per la prevenzione della corruzione e della trasparenza (d'ora in avanti, PTPCT), prestando a tal fine la più ampia collaborazione al RPCT.
2. Il personale rispetta le prescrizioni contenute nel PTPCT; in particolare, rispetta tutte le scadenze in esso contenute.
3. I dipendenti sono tenuti a collaborare con il RPCT, fornendogli tempestivamente tutti i dati e le informazioni richiesti.
4. Eventuali violazioni del dovere di collaborazione con il RPCT costituiscono condotte particolarmente gravi.
5. Il dipendente, fermo restando l'obbligo di denuncia all'autorità giudiziaria, segnala al RPCT, oppure all'Anac utilizzando il canale riservato, le condotte illecite di cui sia venuto a conoscenza che integrino delitti contro la pubblica amministrazione di cui al titolo II, capo I, del codice penale; inoltre, gli altri illeciti rispetto ai quali si riscontri un abuso di potere da parte di un dipendente pubblico al fine di ottenere vantaggi privati così come previsto nel MOG e nelle linee guida Segnalazione illeciti (Whistleblowing). Le altre tipologie di illecito, invece, sono oggetto di segnalazione al superiore gerarchico.
6. Il RPCT cura e verifica la concreta applicazione dei meccanismi di protezione dei dipendenti, previsti dall'articolo 54-*bis* del decreto legislativo n. 165 del 2001 a tutela di chi abbia segnalato condotte illecite nell'interesse dell'integrità della Società.

Art. 10. Trasparenza

1. Il personale, nell'ambito delle proprie attività, è tenuto a fornire, in modo regolare e completo, le informazioni, i dati e gli atti oggetto di pubblicazione sul sito istituzionale, secondo le previsioni contenute nel PTPCT.
2. Il dipendente segnala al Direttore tecnico di appartenenza le eventuali esigenze di aggiornamento, correzione e integrazione delle informazioni, dei dati e degli atti oggetto di pubblicazione, attinenti alla propria sfera di competenza.

Art. 11. Comportamento nei rapporti privati

1. Nei rapporti privati, comprese le relazioni extralavorative con pubblici ufficiali nell'esercizio delle loro funzioni, il personale non sfrutta, né menziona la posizione che ricopre nella Società per ottenere utilità.
2. Il personale non riceve utenti per discutere pratiche di lavoro in luoghi diversi da quelli istituzionalmente previsti.
3. Il personale si astiene dal rendere pubblico con qualunque mezzo (compresi il web, i social network, i blog e i forum) commenti, informazioni, foto, video o audio che possano ledere l'immagine della Società, l'onorabilità dei

colleghi, nonché la riservatezza o la dignità delle persone. La lesione dell'immagine della Società, operata tramite tali mezzi è particolarmente grave quando i giudizi sono resi possibili da informazioni assunte nell'esercizio delle proprie funzioni.

4. Il personale, nei rapporti con le amministrazioni pubbliche, non si accorda per porre in essere scambi di favori, purché non abbiano ad oggetto attività legittimamente poste in essere allo scopo di perseguire al meglio l'interesse affidato ai rispettivi uffici. In nessun caso chiede o accetta raccomandazioni e non presenta persone, né accetta che persone gli siano presentate.
5. Il personale non avvantaggia o danneggia in alcun modo i competitori in procedure comparative, né facilita terzi nel rapporto con il proprio o con altri uffici della Società.
6. Il personale non partecipa a titolo personale a convegni, seminari o tavole rotonde, aventi a oggetto l'attività della Società, senza avere prima informato il Direttore tecnico di riferimento.
7. Il dipendente evita di accettare inviti a occasioni conviviali basate sulla circostanza dell'appartenenza all'organizzazione della Società.

Art. 12. Comportamento in servizio

1. I Direttori tecnici vigilano affinché il personale non adotti comportamenti tali da far ricadere su colleghi il compimento di attività o l'adozione di decisioni di propria spettanza.
2. I Direttori tecnici hanno l'obbligo di controllare che l'uso dei permessi di astensione dal lavoro da parte del personale avvenga effettivamente per le ragioni e nei limiti previsti dalla legge; vigilano, inoltre, sulla corretta timbratura delle presenze, segnalando tempestivamente eventuali irregolarità all'Ufficio del personale.
3. Il personale s'impegna a mantenere la funzionalità e il decoro dell'ufficio, anche assicurando che la propria postazione di lavoro sia in ordine. Si prende, inoltre, cura degli oggetti e degli strumenti che utilizza, attuando le accortezze necessarie al mantenimento della loro efficienza e integrità; in caso di inefficienza, guasto o deterioramento delle risorse materiali e strumentali affidategli, ne dà immediata comunicazione al Direttore tecnico di riferimento. Evita sprechi e diseconomie nel consumo e nell'utilizzo dei beni della Società, e persegue il risparmio energetico.
4. Il personale non attende, durante l'orario di lavoro, a occupazioni estranee al servizio, quali le ripetute conversazioni telefoniche private; inoltre, non accede ai social network, salvo che del tutto sporadicamente e attraverso il personale telefono cellulare. Tale accesso non è mai consentito in presenza di soggetti terzi rispetto alla Società.
5. Il personale si adopera per contrastare il fenomeno del mobbing e provvede a segnalare tempestivamente le condotte che potrebbero integrarlo.
6. Il personale cura la correttà e completa stesura degli atti di propria competenza, in particolare assicurandosi che da essa si evinca con chiarezza il percorso logico-giuridico seguito per giungere alla decisione adottata.
7. Il dipendente si presenta in servizio avendo cura della propria persona e con un abbigliamento consono alle mansioni da svolgere.
8. Il personale non espone negli uffici materiale di natura pubblicitaria che possa denotare una mancanza di imparzialità, di propaganda politica, o comunque sconveniente.

Art. 13. Rapporti con il pubblico e gli organi di informazione

1. Il personale deve essere esaustivo nel fornire le risposte alle varie istanze e reclami ricevuti. Se l'istanza è formulata per posta elettronica, utilizza lo stesso strumento per la risposta, a meno che l'istanza contenga elementi per i quali sia necessario utilizzare altre forme. Occorre che sia sempre identificato o identificabile l'autore della risposta. Istanze e reclami, qualora non determinino l'attivazione di procedimenti amministrativi, sono esitati entro trenta giorni, salvo giustificato motivo.
2. Il personale opera in modo da facilitare gli utenti nello svolgimento dell'attività amministrativa e fornisce agli interessati le informazioni necessarie sulle modalità di presentazione di istanze rientranti nella propria sfera di competenza.
3. Il personale risponde alle telefonate in modo da identificare se stesso e l'ufficio di appartenenza.
4. Il personale che svolge attività lavorativa a contatto con l'utenza si fa riconoscere attraverso l'esposizione in modo visibile del badge o di altro supporto identificativo messo a disposizione dalla società, cura il rispetto degli standard di qualità e di quantità fissati dalla società, ed opera per assicurare la continuità del servizio; mantiene

un comportamento corretto con i colleghi evitando qualsiasi alterco; comunica con gli utenti in modo semplice e comprensibile, evitando un linguaggio eccessivamente specialistico e burocratico.

5. Il personale non assume impegni né anticipa l'esito di decisioni o azioni proprie o altrui inerenti all'ufficio, al di fuori dei casi consentiti. Fornisce informazioni e notizie relative ad atti od operazioni amministrative, in corso o concluse, nelle ipotesi previste dalle disposizioni di legge e regolamentari in materia di accesso.
6. I rapporti con i mezzi di informazione, aventi a oggetto gli argomenti istituzionali, sono tenuti dall'Amministratore Unico e per suo conto dai Direttori Tecnici. Il restante personale, nell'esercizio delle proprie funzioni, non è legittimato a intrattenere rapporti con i mezzi di comunicazione e a rilasciare dichiarazioni o interviste, se non espressamente autorizzato. Il diritto di esprimere valutazioni e di diffondere informazioni a tutela dei diritti sindacali e politici non consente al personale di rilasciare dichiarazioni pubbliche offensive nei confronti della società.
7. La diffusione al pubblico da parte del singolo dipendente tramite e mail, social network, smartphone o altri canali di comunicazione di notizie e immagini relative al proprio lavoro, alle opere eseguite o in corso, deve essere autorizzata, salvo non sia motivata da ragioni di assoluta necessità e urgenza e abbia l'esclusiva finalità di favorire la pubblica incolumità. Tali atti in ogni caso ricadono nell'ambito di responsabilità personale di chi ha diffuso il messaggio o le immagini.

Art. 14. Disposizioni particolari per i dirigenti[7])

1. Le comunicazioni rese dal dirigente ai sensi dell'articolo 13, comma 3 ([8]), del codice generale, sono presentate mediante autocertificazione; in esse, il dirigente s'impegna anche a informare l'amministrazione in caso di successive variazioni.
2. Il dirigente ha l'obbligo di osservare e vigilare sul rispetto delle regole in materia di incompatibilità, cumulo degli impieghi e incarichi di lavoro da parte del personale, al fine di evitare pratiche illecite di "doppio lavoro", anche ai sensi di quanto previsto dal decreto legislativo 8 aprile 2013, n. 39.
3. Il dirigente vigila affinché non si verifichino fenomeni di mobbing e si accerta che il personale alle proprie dipendenze ottemperi alla prescrizione di cui all'articolo 12, comma 5 del presente codice.

Art. 15. Contratti e altri atti negoziali

1. Il dipendente comunica al Direttore tecnico di riferimento ogni situazione di conflitto d'interessi che venga in rilievo nello svolgimento di procedure di aggiudicazione degli appalti e delle concessioni; il conflitto rileva rispetto al personale che interviene nello svolgimento della procedura, o che comunque possa influenzare in qualsiasi modo il risultato.
2. La segnalazione che il dipendente, il quale intenda concludere accordi o negozi, ovvero stipulare contratti a titolo privato, con persone fisiche o giuridiche private con le quali abbia concluso, nel biennio precedente, contratti di appalto, fornitura, servizio, finanziamento ed assicurazione per conto dell'amministrazione, deve rendere al proprio capo ufficio ai sensi dell'articolo 14, comma 3 del codice generale, deve essere preventiva rispetto alla conclusione del negozio.
3. Il dipendente informa il Direttore tecnico di riferimento prima di concludere, per conto della società, ai sensi dell'articolo 1342 del codice civile ([9]), contratti di appalti, fornitura, servizi, finanziamento o assicurazione, con imprese con le quali nel biennio precedente abbia stipulato a titolo privato contratti o ricevuto altre utilità. Allo stesso modo, qualora, nelle forme del citato articolo 1342, intenda concludere a titolo privato accordi, negozi o contratti, con persone fisiche o giuridiche private con le quali nel biennio precedente abbia stipulato per conto della società contratti di appalto, fornitura, servizio, finanziamento ed assicurazione.

[7] Art. 13, comma 1 *DPR 16 aprile 2013 n. 62. Ferma restando l'applicazione delle altre disposizioni del Codice, le norme del presente articolo si applicano ai dirigenti, ivi compresi i titolari di incarico ai sensi dell'articolo 19, comma 6, del decreto legislativo n. 165 del 2001 e dell'articolo 110 del decreto legislativo 18 agosto 2000, n. 267, ai soggetti che svolgono funzioni equiparate ai dirigenti operanti negli uffici di diretta collaborazione delle autorità politiche, nonché ai funzionari responsabili di posizione organizzativa negli enti privi di dirigenza.*

[8] Art. 13, comma 3: *"Il dirigente, prima di assumere le sue funzioni, comunica all'amministrazione le partecipazioni azionarie e gli altri interessi finanziari che possano porlo in conflitto di interessi con la funzione pubblica che svolge e dichiara se ha parenti e affini entro il secondo grado, coniuge o convivente che esercitano attività politiche, professionali o economiche che li pongono in contatti frequenti con l'ufficio che dovrà dirigere o che siano coinvolti nelle decisioni o nelle attività inerenti all'ufficio. Il dirigente fornisce le informazioni sulla propria situazione patrimoniale e le dichiarazioni annuali dei redditi soggetti all'imposta sui redditi delle persone fisiche previste dalla legge"*

[9] *Articolo che disciplina i contratti per adesione.*

4. Se nelle situazioni indicate ai commi 1, 2 e 3 si trovano i Direttori tecnici, essi indirizzano l'informazione al RPCT.
5. Il personale che partecipa alle procedure di gara segnala tempestivamente al proprio superiore gerarchico eventuali proposte ricevute da concorrenti o dall'aggiudicatario, aventi a oggetto utilità di qualunque tipo in favore proprio, dei suoi parenti o affini entro il secondo grado, del coniuge o del convivente.
6. Nei confronti degli operatori economici che concorrono alle gare d'appalto e degli aggiudicatari di contratti, il personale limita i contatti a quelli strettamente indispensabili alla trattazione delle pratiche di ufficio.
7. Il personale che partecipa alle procedure di gara mantiene la riservatezza in merito all'intera procedura ed evita situazioni anche solo percepite di conflitto di interessi.

Art. 16. Disposizioni particolari per i componenti delle commissioni esaminatrici

1. Il personale componente delle commissioni esaminatrici, nonché i segretari, sono tenuti a mantenere assoluta riservatezza sulle operazioni svolte, sui criteri di valutazione adottati e sulle determinazioni raggiunte.
2. Il personale componente delle commissioni esaminatrici è tenuto a verbalizzare qualsiasi irregolarità rilevata.

Art. 17. Disposizioni finali

1. Il RPCT assicura che, ai sensi dell'articolo 17, comma 2 ([10]) del codice generale, sia data la più ampia diffusione al presente codice, mediante pubblicazione sul sito internet istituzionale e sulla rete intranet, nonché tramite e-mail inviata a tutto il personale in servizio, nonché ai titolari di contratti di consulenza o collaborazione a qualsiasi titolo, anche professionale, nonché ai collaboratori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore della Società.
2. Copia del presente codice viene consegnata e fatta sottoscrivere ai nuovi assunti, con rapporti comunque denominati, contestualmente alla stipulazione del contratto di lavoro o, in mancanza, all'atto di conferimento dell'incarico.

[10] Articolo 17, comma 2: *"Le amministrazioni danno la più ampia diffusione ai codici di comportamento da ciascuna definiti ai sensi dell'articolo 54, comma 5, del citato decreto legislativo n. 165 del 2001 secondo le medesime modalità previste dal comma 1 del presente articolo"*