COPIA

UNIONE DEI COMUNI

"ARO 2 Barletta Andria Trani"

Deliberazione della Giunta

Nr. 27

OGGETTO: Adozione del Regolamento interno per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche con riguardo al trattamento dei dati personali – Regolamento UE 2016/679

L'anno duemila **diciotto** il giorno **ventinove** del mese di **novembre** alle ore **12.40** in Andria, presso la Sala Giunta della Sede Municipale, si è riunita, previa convocazione trasmessa ai Sindaci, componenti dell'ARO2, la Giunta dell'Unione dei Comuni dell'ARO2.

Risultano presenti ed assenti i sotto indicati componenti :

Comune	*Presenti*	*Assenti*	*Rappresentante*
Andria	*1*		*Nicola GIORGINO – Sindaco*
Canosa di Puglia	*2*		*Roberto MORRA - Sindaco*
Minervino Murge	*3*		*Maria Laura MANCINI - Sindaco*
Spinazzola	*4*		*Michele PATRUNO - Sindaco*

Assume la presidenza l'avv. Nicola GIORGINO, Presidente dell'ARO2, il quale, preso atto della validità della adunanza - regolarmente convocata con nota prot. 1315 del 22/11/2018, dichiara aperta la seduta.

Partecipa per le funzioni verbalizzanti il Segretario Generale Dott. Giuseppe Borgia.
Sono presenti i Dirigenti dell'ARO Dott.ssa Maria De Palma e Ing. Antonio Dibari.

LA GIUNTA DELL'UNIONE

PRESO ATTO che :

- il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;

- il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento, prevista il 25 maggio 2018;

- ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;

- in data 19/09/2018 è entrato in vigore il Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

RILEVATO che :
- la rapida diffusione delle nuove tecnologie informatiche con libero accesso alla rete Internet da dispositivi di vario tipo quali personal computer, tablet, smartphonet etc.., espone la Rete Informatica dell'Unione dei Comuni ARO 2 BAT , a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (Disciplina sulla protezione dei dati personali e sul Diritto d'autore), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso;
- quindi 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;
- a tal fine si rende opportuno adottare un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati personali, indicando prescrizioni specifiche per il personale dell'Ente;

Visto lo schema di Regolamento allegato;

RITENUTO pertanto opportuno procedere alla sua approvazione;

Tanto premesso,

Acquisito il parere di regolarità tecnica espresso ai sensi dell'art. 49 c. 1 D.Lg 267/2000;

Con voti unanimi favorevoli

DELIBERA

- Di approvare il Regolamento interno per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche con riguardo al trattamento dei dati personali – Regolamento UE 2016/679, allegato al presente atto per costituirne parte integrante e sostanziale.

ALLEGATO ALLA PROPOSTA DI

DELIBERAZIONE DI GIUNTA DELL'UNIONE

avente ad

OGGETTO:Adozione del Regolamento interno per l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche con riguardo al trattamento dei dati personali – Regolamento UE 2016/679

PARERI DI REGOLARITA' AI SENSI DELL'ART. 49 del D.Lg.vo n° 267/2000

****

Ai sensi dell'art. 49, 1° comma del D.Lg.vo n° 267/2000, sulla presente proposta si esprime il seguente parere sotto il profilo della **REGOLARITA' TECNICA**:

favorevole

Lì, 19/09/18

IL RESPONSABILE DEL SERVIZIO
f.to Dott.ssa Maria De Palma

REGOLAMENTO INTERNO PER L'UTILIZZO E LA GESTIONE DELLE RISORSE STRUMENTALI INFORMATICHE E TELEMATICHE

UNIONE DI COMUNI ARO 2 BARLETTA ANDRIA TRANI

Sommario

Premessa

La rapida diffusione delle nuove tecnologie informatiche con libero accesso alla rete Internet da dispositivi di vario tipo quali personal computer, tablet, smartphonet etc.., espone *la Rete* Informatica dell' Unione dei Comuni ARO 2 BAT (d'ora in avanti Ente), a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (Disciplina sulla protezione dei dati personali e sul Diritto d'autore), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso.

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, l'Ente **adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati personali.**

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutto il personale dell'Ente, nonché integrano le informazioni fornite agli interessati in Ente alle ragioni ed alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

1. Campo di applicazione

Il presente Regolamento disciplina l'utilizzo e la gestione delle risorse strumentali informatiche e telematiche nella disponibilità dell'Ente e si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell'Ente, a prescindere dal rapporto contrattuale con lo stesso intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "**utente**" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche essere indicata quale "**soggetto autorizzato al trattamento dei dati**" come previsto dal Regolamento UE 2016/679.

2. Utilizzo del Personal Computer

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 evitando ogni possibile forma di danneggiamento.

Il Personal Computer dato in affidamento all'utente, permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione.

Il personale incaricato in qualità di *Amministratore di Sistema* è 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.). Detti interventi, in considerazione dei divieti di cui ai successivi punti, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento del dipendente.

Il personale tecnico autorizzato ha facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni di lavoro, nel rispetto della Disciplina in materia di protezione dei dati personali, 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, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso previo consenso dell'interessato.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale autorizzato dall'Ente, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Ente a gravi 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 anche penalmente.
Salvo preventiva espressa autorizzazione del Responsabile della protezione dei dati aziendali, 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, Internet key ...).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile della protezione dei dati nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto n° 11 del presente Regolamento relativo alle procedure di protezione antivirus.

Non è consentito collegare alla rete aziendale Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo Hardware senza l'autorizzazione del Responsabile della protezione dei dati o del Titolare del trattamento.

3. Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla Rete informatica dell'Ente vengono inizialmente assegnate dal personale tecnico autorizzato e successivamente reimpostate dal dipendente stesso secondo criteri prestabiliti e vigenti disposizioni normative.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata e creata dall'incaricato che dovrà essere memorizzata, custodita con la massima diligenza e non divulgata.

La parola chiave deve essere formata da almeno otto caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali, anche in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password di accesso di ciascun incaricato dovrà essere reimpostata ogni tre mesi.
In base a tale procedura (manuale o automatizzata), il dipendente dovrà inserire ogni 3 mesi una password nuova, diversa dalla precedente, che non dovrà condividere con nessun collega.

L'utente potrà richiedere la modifica della parola chiave (reset password) al Titolare del trattamento o al Responsabile della protezione dei dati, per decorrenza del termine sopra previsto e/o in caso di perdita della riservatezza. In caso di mancato utilizzo dell'utenza di accesso al Pc per oltre 6 mesi, l'account sarà automaticamente bloccato per sicurezza aziendale.

4. Utilizzo della Rete

Per l'accesso alla rete informatica dell'Ente ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente di un altro collega. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

La presenza di eventuali cartelle di rete condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.
Tutti i dischi fissi dei Pc o altre unità di memorizzazione locali (es. disco C:\ del proprio PC) non sono soggetti a salvataggio da parte del personale autorizzato.
La responsabilità del salvataggio dei dati eventualmente ivi contenuti è pertanto a carico del singolo dipendente o collaboratore, in qualità di soggetto autorizzato al trattamento.

Il Responsabile della protezione dei dati potrà in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer sia sulle unità di rete informatica aziendale, previa conferma del Titolare del trattamento.

5. Utilizzo e conservazione dei supporti rimovibili

Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi o cassetti chiusi a chiave.

E' vietato il trasporto di supporti rimovibili, contenenti dati aziendali, all'esterno della struttura aziendale. Inoltre non è ammesso qualsiasi altro punto di archiviazione dati aziendali tramite internet (i.e. web storage), se non espressamente autorizzato dal Responsabile della protezione dei dati o dal Titolare.

L'utente è responsabile della custodia dei supporti e dei dati personali in essi contenuti.

6. Utilizzo di PC portatili

L'utente è responsabile del computer portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

Ai computer portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

I computer portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Tali disposizioni si applicano anche nei confronti di collaboratori e consulenti esterni.

E' vietato connettersi alla rete informatica dell'Ente attraverso qualsiasi dispositivo personale (smart phone etc.) non preventivamente autorizzato dal Responsabile della protezione dei dati o dal Titolare.

7. Dismissioni Supporti

In caso di dismissione di supporti di memoria (hard-disk etc..) che contengono dati personali, il Responsabile della protezione dei dati dovrà disporre idonei accorgimenti e misure volte a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate ad essere reimpiegate, riciclate o smaltite.

Chiunque procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti interni, acquisendo attraverso apposita modulistica, l'autorizzazione a cancellarli o a renderli non intelligibili.

8. Uso della posta elettronica

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.

È fatto divieto di utilizzare le caselle di posta elettronica 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. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

È obbligatorio prestare la massima attenzione nell'aprire i file allegati alle e-mail prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Nel caso in cui un utente di posta si assenti per più giorni (p.es. per malattia), sarà consentito al superiore gerarchico dell'utente o comunque, previa autorizzazione dello stesso, a persona individuata dal responsabile d'ufficio, accedere alla casella di posta elettronica, al fine di garantire la continuità lavorativa e comunque, nel rispetto del principio di necessità e di proporzionalità.

Il Titolare del trattamento, nella persona del Presidente dell'Ente, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica del collaboratore per le sole finalità di garanzia della continuità di servizio istituzionale, ove ritenuto indispensabile.

Le caselle di posta elettronica istituzionale nominative (nome.cognome@) hanno validità pari alla durata della permanenza in servizio del collaboratore.
Nel caso il cui il collaboratore non presti più la sua attività lavorativa presso l'Ente, la casella di posta elettronica sarà prontamente disattivata. Su richiesta dell'interessato la casella di posta potrà restare attiva per ulteriori due mesi dalla data di cessazione del rapporto di lavoro, durante il quale l'interessato provvederà ad inserire una risposta automatica d'ufficio.

9. Navigazione in Internet

Il Personale computer assegnato al collaboratore ed abilitato alla navigazione in Internet costituisce uno strumento 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 all'interno dell'Ente.

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

- l'upload o il download di software gratuiti (freeware) e shareware;
- l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica);
- 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 dal Titolare 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'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Titolare;
- l'accesso, tramite internet, a caselle web-mail di posta elettronica personale.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ente rende peraltro nota l'adozione di uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'accesso a determinati siti non istituzionali inseriti in una specifica *black-list* dinamica.

Gli eventuali controlli per motivi di sicurezza, compiuti da personale autorizzato dall'Ente, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui log non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questo Ente.

10. Protezione antivirus

Il sistema informatico dell'Ente è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer, nonché segnalare prontamente l'accaduto al Presidente e al Responsabile della protezione dei dati.

Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Responsabile della protezione dei dati o al Presidente.

11. Accessi Remoti

Gli accessi da remoto verso la rete informatica dell'Ente possono essere effettuati solo previa autorizzazione del Presidente o del Responsabile della protezione dei dati. Tutti gli accessi sono monitorati e registrati. Non sono ammessi accessi di tipologia differente da quella definita dal Presidente. A seguito conclusione o risoluzione del rapporto di collaborazione con l'utente, l'accesso remoto sarà prontamente disabilitato.

12. Utilizzo di apparecchiature fuori sede

Qualora venisse assegnato un dispositivo aziendale (*ad es.* cellulare, smartphone, tablet etc..) al dipendente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. E' vietato l'utilizzo dei dispositivi per inviare sistematicamente comunicazioni di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
Ai computer portatili si applicano le regole di utilizzo previste per i computer connessi in rete aziendale con particolare attenzione alla rimozione di eventuali file personali elaborati sullo stesso prima della riconsegna. Il computer portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files di lavoro strettamente necessari. L'utente provvederà a collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus e del sistema operativo aziendale.

13. Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali e di misure adeguate di sicurezza, come indicato nella lettera di designazione del Presidente, a soggetto autorizzato al trattamento.

14. Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Presidente accedere direttamente, nel rispetto della vigente disciplina in materia di protezione dei dati personali, a tutti gli strumenti informatici dell'Ente e ai documenti ivi contenuti.

15. Obbligo riservatezza e tutela Cliente

Il Collaboratore è rigorosamente tenuto ad osservare la massima riservatezza in relazione ad atti, fatti, cognizioni, documenti, prototipi e su tutte le informazioni, nella più ampia accezione del termine, acquisite nel corso delle attività o delle quali il dipendente è comunque venuto a conoscenza. Nel caso di inadempimento dei predetti obblighi, l'Ente potrà procedere alla risoluzione del contratto, salvo il diritto all'ulteriore risarcimento del danno, in ossequio alle vigenti disposizioni di legge in materia.

16. Sistemi di controlli graduali

In caso di anomalie sulla rete informatica dell'Ente, il personale tecnico autorizzato dal Presidente effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'ufficio in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

17. Sanzioni

E' fatto obbligo a tutti i dipendenti e collaboratori dell'Ente di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

18. Aggiornamento e revisione

Tutto il personale dell'Ente potrà proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

19. Entrata in vigore del regolamento e pubblicità

Con l'entrata in vigore del presente Regolamento, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

Del che si è redatto il presente verbale che, previa lettura e conferma, viene sottoscritto.

IL PRESIDENTE
F.to avv. Nicola GIORGINO

IL SEGRETARIO VERBALIZZANTE
F.to Dott. Giuseppe Borgia

Copia conforme all'originale, in carta libera per uso amministrativo.

Li, 13 DIC. 2018

UNIONE DI COMUNI ARO 2 BT

IL SEGRETARIO GENERALE
Dott. Giuseppe BORGIA

Prot. N. _____

Della suestesa deliberazione viene iniziata oggi la pubblicazione all'Albo del Comune di _____ _____ per 15 giorni consecutivi.

Addì 13 DIC. 2018 _____

UNIONE DI COMUNI ARO 2 BT

IL SEGRETARIO GENERALE

IL SEGRETARIO GENERALE
Dott. Giuseppe BORGIA

ADEMPIMENTI RELATIVI ALLA PUBBLICAZIONE

Il Responsabile del procedimento, visti gli atti d'ufficio

ATTESTA

Che la presente deliberazione:

> è stata affissa all'Albo Pretorio comunale per 15 giorni consecutivi a partire dal _____ al _____ come prescritto dall'art. 124 comma 1°, del D.Lg.vo n° 267 del 18/8/2000.

> è divenuta esecutiva perchè:
- decorsi 10 giorni dalla pubblicazione (art. 134 comma 3) del D.Lg.vo n° 267 del 18/8/2000
- dichiarata immediatamente eseguibile (art. 134 comma 4) del D.Lg.vo n° 267 del 18/8/2000.

_____ _____

Addi'

_____