COPIA

COMUNE DI BAULADU

PROVINCIA DI ORISTANO

Via Arruga Antoni Gramsci n. 7 – 09070 Bauladu (OR) Tel. 078351677- 078351678

P.IVA 00072000953

Sito Internet: www.comune.bauladu.or.it – Email: tecnico@comune.bauladu.or.it

Determinazione Area Tecnica

Numero 73 del 10-12-2018

Oggetto:	**DESIGNAZIONE DEGLI AUTORIZZATI INTERNI AL TRATTAMENTO DEI DATI PERSONALI, AI SENSI DELL'ART. 29, RGPD.**

IL RESPONSABILE DEL SERVIZIO

Visto il Decreto del Sindaco n° 4 del 23.10.2018 con il quale è stato nominato Responsabile del Settore Amministrativo;

Richiamate le deliberazioni di seguito riportate:

- C.C. n° 6 del 31.01.2018 avente ad oggetto: "Approvazione del Bilancio di Previsione Finanziario 2018/2020 (Art. 151 D.Lgs. 267/2000 e Art. 10 D.Lgs. n° 118/2011) e successive modificazioni ed integrazioni;
- G.M. n° 10 del 09.02.2018 relativa all'approvazione del Piano Operativo di Gestione 2018/2020 e successive modificazioni ed integrazioni;

Considerato che:

- Con delibera C.C. n. 1 del 31.01.2013 è stato approvato il Regolamento Comunale per la Disciplina dei Controlli Interni;
- Con Delibera G.C. n. 3 del 22.01.2014 è stato approvato il Codice di Comportamento dei Dipendenti del Comune di Bauladu;
- Con Delibera G.C. n° 6 del 09.02.2018 è stato approvato il Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza PTPCT 2018/2020;
- Non sussistono situazioni di incompatibilità di cui all'art. 53 del Decreto legislativo 165/2001 e successive modificazioni ed integrazioni;

Premesso che:

- in data 25 maggio 2018, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE il 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (di seguito RGPD);
- ai sensi dell'art.4, paragrafo 1, punto 7), RGPD 2016/679, per Titolare del trattamento si intende la persona fisica o giuridica,l'autorità pubblica, il servizio o l'organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Nel caso di una Pubblica Amministrazione, il Titolare del trattamento dei dati è l'Ente nel suo complesso;

- Con decreto sindacale n. 5 del 26.10.2018 il Sindaco pro tempore, nella sua qualità di legale rappresentante dell'Ente, ha individuato il sottoscritto quale Responsabile del trattamento dei dati per l'Area TECNICA;
- l'art. 29, RGPD, prevede che "chiunque abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento" ovvero dal Responsabile del trattamento;
- il richiamato art. 29, RGPD, prevede che le operazioni di trattamento possano essere effettuate solo da soggetti che operino sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite;
- con deliberazione della Giunta Comunale n. 77 del 25.10.2010 è stata approvata la Pianta organica dell'ente suddivisa per Aree e Servizi;
- si rende necessario procedere alla formale ed espressa individuazione delle persone fisiche (Autorizzate al trattamento) interne all'Ente che saranno autorizzate al trattamento dei dati personali nell'ambito dell'AREA TECNICA come di seguito riportato:

1. SUAP - EDILIZIA PRIVATA (Geom. Masala Angelo);
2. Polizia Mortuaria e Sevizi Cimiteriali (Sig. Murru Alfredo);
3. Polizia Mortuaria e Servizi Cimiteriali (Sig. Ghiani Salvatore);

con particolare riferimento alle Banche Dati trattate dai Singoli Uffici/Servizi;

- le persone fisiche autorizzate, effettueranno il trattamento dei dati, attenendosi scrupolosamente alle istruzioni impartite dal Responsabile del trattamento;

Visti i singoli procedimenti amministrativi di pertinenza dell'Ufficio, le Banche Dati cartacee e/o informatiche trattate per la gestione dei procedimenti amministrativi di competenza;

Considerato che il Responsabile del procedimento cura, nei termini di legge, gli adempimenti previsti dall'art. 6 della Legge 241/90 e successive modifiche e che l'elencazione delle attività e competenze più sopra citate non è esaustiva ma solo esemplificativa, rientrando nelle stesse anche tutte le attribuzioni complementari, funzionali e necessarie per la formazione dell'atto finale e tutti i procedimenti non indicati ma inerenti il servizio attribuito, nonché di quanto espressamente assegnato, volta per volta dal responsabile dell'Area.

Visti:
- il combinato disposto di cui agli artt. 107 e 109 del T.U. degli Enti Locali, approvato con D.Lgs. 18.08.2000, n. 267;
- il vigente regolamento comunale in materia di funzionamento degli uffici e dei servizi;

Dato atto che:
- ✓ L'istruttoria ai fini dell'adozione del presente provvedimento è stata espletata dal sottoscritto Responsabile;
- ✓ ai sensi dell'art. 6 bis della 241/1990 s.m.i. non è stata rilevata la presenza di situazioni di conflitto di interesse;
- ✓ il procedimento amministrativo si è svolto nel rispetto del vigente:
  - ✓ Piano Triennale della Trasparenza e Integrità, adottato ai sensi dell'art. 10 del D.Lgs n. 33/2013;
  - ✓ Piano della Prevenzione della Corruzione nella Pubblica Amministrazione adottato ai sensi della Legge 190/2012;
  - ✓ Codice di Comportamento dei Dipendenti del Comune di Bauladu, adottato ai sensi del DPR 62/2013;

Dato atto, altresì, che ai sensi e per gli effetti di quanto disposto dall'art. 147/bis, comma 1 , del Decreto legislativo 267/2000, il presente provvedimento verrà sottoposto

al controllo secondo le modalità disciplinate nel Regolamento Comunale per la Disciplina dei Controlli Interni;

DETERMINA

Di designare quali autorizzati interni al trattamento dei dati personali dell'Area Tecnica i dipendenti:

Cognome Nome e servizio di riferimento	Responsabile del Procedimento		Inquadramento Giuridico
	SI	NO	
Masala Angelo - Istruttore Tecnico: SUAP, Edilizia Privata	X		Categoria C
Murru Alfredo - Operaio: Polizia Mortuaria e Servizi Cimiteriali		X	Categoria A
Ghiani salvatore - Operaio: Polizia Mortuaria e Servizi Cimiteriali		X	Categoria A

Di dare atto che l'elencazione delle attività e competenze più sopra citate non è esaustiva ma solo esemplificativa, rientrando nelle stesse anche tutte le attribuzioni complementari, funzionali e necessarie per la formazione dell'atto finale e tutti i procedimenti non indicati ma inerenti il servizio attribuito, nonché di quanto espressamente assegnato, volta per volta dal responsabile dell'Area.

Di dare altresì atto che in ottemperanza al RGPD, che disciplina la protezione delle persone fisiche con riferimento al trattamento dei dati personali, gli incaricati sono autorizzati a trattare i dati personali, nonché le eventuali categorie particolari di cui agli artt. 9 e 10 del GDPR, strettamente necessari per l'istruttoria e la definizione dei procedimenti amministrativi di competenza dell'Ufficio/Servizio, secondo le indicazioni di seguito elencate:

I dipendenti individuati quali Autorizzati al trattamento dei dati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali personali di autenticazione al sistema, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperta la propria sessione di lavoro in caso di allontanamento anche temporaneo dalla postazione informatica, al fine di evitare trattamenti non autorizzati o non consentiti e di rendere possibile, in qualunque momento, l'individuazione dell'autore materiale del trattamento;
- conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza ed il dovuto riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali con riferimento alla gestione dei procedimenti amministrativi di competenza dell'Ufficio/Servizio;
- custodire e controllare i dati personali affidati affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare nuove banche dati senza autorizzazione espressa del Responsabile del trattamento dei dati;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente, in conformità alle disposizioni impartite dal Responsabile del trattamento dei dati come di seguito dettagliate;
- fornire al Responsabile del trattamento dei dati tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Con riferimento all'utilizzo della postazione di lavoro assegnata in uso:

- Il Personal Computer (PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi ulteriori di manutenzione e minacce alla sicurezza dei dati trattati dall'Ente.
- I dipendenti devono custodire la propria strumentazione in modo diligente, segnalando con tempestività ogni danneggiamento, avaria, furto o smarrimento al Responsabile del trattamento.
- L'accesso a ciascun PC è protetto da credenziale di autenticazione costituita da una User ID (codice per l'identificazione dell'autorizzato) associata ad una PASSWORD (parola chiave), quest'ultima, conosciuta esclusivamente dal medesimo autorizzato.
- Gli autorizzati del trattamento dei dati sono responsabili della custodia e dell'utilizzo diligente e consapevole delle proprie credenziali di autenticazione che devono essere gestite attenendosi alle seguenti istruzioni:
    a) La password assegnata a ciascun autorizzato, è composta da un numero minimo di otto caratteri e almeno tre delle seguenti caratteristiche:
    -Lettere maiuscole;
    -Lettere minuscole;
    -Numeri;
    -Caratteri speciali.
    b) La password assegnata, deve essere prontamente e autonomamente sostituita dall'autorizzato al primo accesso al sistema e successivamente modificata con cadenza almeno trimestrale.
    c) La password deve essere consegnata, in busta chiusa e sigillata, al Responsabile del trattamento dei dati affinché proceda alla custodia delle credenziali.
    d) La password non deve contenere riferimenti, diretti o indiretti, agevolmente riconducibili all'autorizzato.
    e) La password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi.
    f) L'autorizzato è responsabile di ogni utilizzo indebito o non consentito del profilo utente di cui sia titolare.
    g) Qualora, in caso di prolungata assenza o impedimento dell'autorizzato, si verificasse la necessità di accedere ai dati ed agli strumenti elettronici a quest'ultimo assegnati in via esclusiva per esigenze di operatività e di sicurezza del sistema, il Responsabile del trattamento dei dati (coincidente con il Responsabile dell'Area) provvede ad eseguire l'accesso autonomamente utilizzando le proprie credenziali di autenticazione –in quanto configurate secondo un profilo di autorizzazione sovraordinato rispetto a quello dei soggetti autorizzati, propri sottordinati gerarchici – redigendo un verbale delle operazioni compiute. In tal modo è garantita la piena tracciabilità dell'accesso che sarà comunque registrato mediante i file di log. Al rientro in servizio dell'autorizzato assente ovvero impedito, il Responsabile del Trattamento dei Dati provvederà ad informarlo dell'accaduto consegnandogli copia del verbale delle operazioni compiute.
    h) Le credenziali di autenticazione individuali per l'accesso all'elaboratore, ovvero ai software applicativi e gestionali, non devono mai essere condivise tra più utenti (anche se autorizzati al trattamento). Se un dipendente dovesse avere la necessità di trattare gli stessi dati o di usare le stesse procedure alle quali può accedere un collega, dovrà chiedere, al Responsabile del trattamento ovvero all'Amministratore di Sistema, che gli sia assegnato uno specifico profilo di autorizzazione per il trattamento di quei dati, ovvero che gli siano assegnate specifiche credenziali di autenticazione, dotate dei privilegi necessari per l'accesso ai dati o ai servizi richiesti.
    i) Se l'autorizzato sospetta che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della propria password.

- Il dipendente autorizzato al trattamento dei dati, preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore nonché l'utilizzo dei relativi servizi in nome del dipendente e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi, si impegna a:

1. non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato;
2. non lasciare incustodita ed accessibile la propria postazione una volta che sia avvenuta l'autenticazione con le proprie credenziali;
3. conservare e custodire la password nella massima riservatezza e con la massima diligenza;
4. non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti casualmente a conoscenza;
5. mantenere la corretta configurazione del proprio elaboratore non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati.

- Qualunque azione o attività posta in essere mediante l'utilizzo del codice identificativo e della password assegnate, è attribuita in via esclusiva al dipendente assegnatario delle credenziali di autenticazione che sarà chiamato a rispondere delle attività eseguite.
- Il dipendente è civilmente responsabile di qualsiasi danno arrecato all'Ente e/o a terzi in violazione di quanto espressamente previsto dalla norma e di quanto indicato nella presente Determinazione.
- Il dipendente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua password (profilo utente).
- La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.
- Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del trattamento e dell'Amministratore di Sistema dell'Ente. In caso di necessità di acquisto o di dotazione di programmi applicativi e procedure, sarà necessario preventivamente richiedere e acquisire l'autorizzazione in forma scritta da parte dell'Amministratore di Sistema dell'Ente, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei Sistemi e della Rete.
- Non è consentito ai dipendenti modificare le impostazioni di sistema sui PC assegnati, come la configurazione di rete e del Browser per la navigazione su internet, salvo esplicita autorizzazione dell'Amministratore di Sistema dell'Ente.
- Il Personal Computer deve essere spento al termine della propria attività lavorativa, prima di lasciare l'ufficio oppure in caso di assenza prolungata dall'ufficio stesso. Lasciare infatti un elaboratore incustodito potrebbe essere causa di utilizzo improprio da parte di terzi senza che per l'Ente ci sia la possibilità di fornire la prova dell'indebito uso.
- Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (pen drive, modem etc.) se non con l'espressa autorizzazione del Responsabile del trattamento dei dati e dell'Amministratore di Sistema dell'Ente.
- Ogni dipendente deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna, avvertendo senza indugio il Responsabile del trattamento dei dati e l'Amministratore di Sistema nel caso in cui si dovesse rilevare la presenza di virus.
- E' vietato utilizzare gli strumenti informatici dell'Amministrazione al fine di custodire, far circolare ovvero promuovere, materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi non licenziati) e ogni altra tipologia di materiale non autorizzato.
- E' vietato copiare, scaricare ovvero mettere a disposizione di altri materiale protetto dalla legge sul diritto di autore (documenti, files musicali, film e filmati) di cui l'Ente non abbia acquisito i diritti.
- E' vietato rimuovere, danneggiare deliberatamente ovvero asportare componenti hardware.
- E' fatto obbligo al dipendente in possesso di software antivirus di mantenere sempre attivo il programma con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in questo senso, è necessario fornire immediata segnalazione al proprio Responsabile del trattamento ed all'Amministratore di Sistema dell'Ente.
- Il dipendente al quale sia stato assegnato dall'Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro.

- Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi alla Rete Locale.

Con riferimento al collegamento ad Internet

- E' vietato l'accesso e l'utilizzo delle risorse di rete in assenza di preventiva autenticazione informatica.
- E' vietato l'utilizzo di modem per l'accesso ad Internet, salvo specifica autorizzazione in tal senso da parte del Responsabile del trattamento e dell'Amministratore di Sistema dell'Ente.
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Ente.
- Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento dell' attività istituzionale. E' pertanto proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
- Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
- E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili salvo i casi espressamente autorizzati o attinenti ai compiti ed alle mansioni assegnate.
- E' vietata ogni forma di registrazione a siti o a mailing list i cui contenuti non siano legati allo svolgimento dell'attività lavorativa istituzionale.
- E' vietata la partecipazione a Forum, chat line, bacheche elettroniche e registrazioni in guest books anche utilizzando pseudonimi (ovvero nicknames), ovvero l'utilizzo di social network, qualora queste attività non siano strettamente attinenti all'attività lavorativa svolta.
- E' vietata tassativamente la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti oltraggiosi, discriminatori ovvero che offendono il comune senso del pudore.
- Al dipendente non è consentito:
  a) servirsi o dar modo ad altri di servirsi della stazione di accesso ad Internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
  b) scaricare software dalla rete se non espressamente autorizzato dal Responsabile del trattamento e dall'Amministratore di Sistema dell'Ente;
  c) utilizzare internet provider diversi da quello ufficiale dell'Ente e connettere stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
  d) usare la rete in modo difforme da quanto previsto dalla presente Determinazione e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servi zi svolti sulla rete.

Con riferimento all'utilizzo dei Supporti Magnetici o Ottici

- non è consentito scaricare files (programmi, archivi di dati, ecc) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- è fatto obbligo di sottoporre a controllo preventivo, tramite scansione antivirus, tutti i files di provenienza incerta o esterna, attinenti all'attività lavorativa.

Con riferimento all'utilizzo della Posta Elettronica

- L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali l'Ente assegna una casella di posta istituzionale (nominativa ovvero per l'Ufficio/Servizio).
- La casella di posta elettronica istituzionale è uno strumento di lavoro che deve pertanto essere utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo. I dipendenti ai quali è assegnata, sono responsabili del corretto utilizzo della stessa.

- E' fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail - list non attinenti la propria attività svolta per l'Ente, salvo diversa esplicita autorizzazione in tal senso.
- La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente i documenti inutili e gli allegati ingombranti.
- E' vietato utilizzare il servizio di posta elettronica istituzionale per inoltrare catene telematiche, appelli, petizioni, giochi, scherzi, barzellette, e altre e- mails che non abbiano attinenza con l'attività lavorativa. Se si dovessero ricevere messaggi di tale tipo, è necessario informare con immediatezza il Responsabile del trattamento e l'Amministratore di Sistema dell'Ente. In ogni caso, è fatto espresso divieto all'autorizzato di aprire gli allegati di tali messaggi.
- E' vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di utenti non istituzionali. E' parimenti vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi, macro, scripts). Si ribadisce che, i soggetti designati come "autorizzati al trattamento" possono accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti ed alle funzioni istituzionali loro assegnate.

Di trasmettere la presente determinazione ai dipendenti interessati per i provvedimenti di competenza;

Di Pubblicare la presente determinazione all'albo pretorio del sito istituzionale www.comune.zeddiani.or.it e nella sezione Amministrazione Trasparente a norma del D.Lgs 33/2013.

IL RESPONSABILE DEL PROCEDIMENTO

F.to Contu Gabriella

IL RESPONSABILE DEL SERVIZIO
F.to Contu Gabriella

ATTESTATO DI PUBBLICAZIONE

Della suestesa determinazione viene iniziata oggi la pubblicazione all'Albo Pretorio on-line per 15 giorni consecutivi dal 10-12-2018 al 25-12-2018.
Lì 10-12-2018

IL RESPONSABILE DEL SERVIZIO
F.to Contu Gabriella

Copia Conforme ad uso amministrativo.

Lì 10-12-2018

IL RESPONSABILE DEL SERVIZIO
Contu Gabriella