ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali del Comune di Motta Sant'Anastasia Ente locale, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso del Comune diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine del Comune.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o

l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti del Comune;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica

delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi del Comune di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
  - Non deve mai essere disattivato;
  - Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
  - Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali del Comune, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature...) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
- quando il PC portatile è all'esterno del Comune, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
- in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi del Comune;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;

• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

• tutela l'utilizzatore ed in generale il Comune da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;

• è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

• devono essere lunghe almeno otto caratteri;

• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;

• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;

• non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

• Almeno ogni 3 mesi è obbligatorio cambiare la password;

• Ogni password ricevuta va modificata al primo utilizzo;

• La password venga conservata in un luogo sicuro;

• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;

• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi personali, o comunque non del Comune, quali lettori dispositivi di memorizzazione dei dati;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete del Comune, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d) Gestione posta elettronica del Comune

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità del Comunee in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza del Comune e di prevenire conseguenze legali a carico

della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

e) Gestione del salvataggio dei dati

• Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
• Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti...). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore del Comune è stato installato un software antivirus del Comune che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus del Comune non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad

esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database del Comune che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso

da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. NON OSSERVANZA DELLA NORMATIVA DEL COMUNE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Dalla residenza Municipale,

Il titolare del trattamento

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche dell'ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Comune di Motta Sant'Anastasia Ente locale ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere al Comune, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dal Comune, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività istituzionale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici comunali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della Comune di Motta Sant'Anastasia Ente locale. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre il Comune a gravi responsabilità civili ed anche penali in caso di violazione 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici comunali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici comunali.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici comunali* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. 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 controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici comunali* 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.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici comunali.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici comunali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici comunali,* nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici comunali.*

UTILIZZO DEI SUPPORTI MAGNETICI
Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati

memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI
L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici comunali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA
La casella di posta, assegnata dalil Comune 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 comunale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Comune di Motta Sant'Anastasia Ente locale deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per il Comune "know how" comunale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, ...).
Per la trasmissione di file all'interno di Comune di Motta Sant'Anastasia Ente locale è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici comunali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI
Il PC abilitato alla navigazione in Internet costituisce uno strumento comunale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici comunali*.
È 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 direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando

pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Dalla residenza Muncipale,

Il titolare del trattamento

All'attenzione di
(indicare il titolare del trattamento)

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a.....
nato/a a.....il....., esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali
(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

- ☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- ☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;
  - le finalità del trattamento;
  - le categorie di dati personali trattate;
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
- ☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:
  a)...;
  b)....;
  c)...;
- ☐ nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;
- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

- ☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- ☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: .....):*
  - ☐ tutti i dati personali forniti al titolare;
  - ☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento
(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto
(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

_____

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.
- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

_____

Recapito per la risposta:
Via/Piazza
Comune Provincia Codice postale
oppure
e-mail/PEC:

Eventuali precisazioni
Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____
_____
_____
_____
_____

(Luogo e data)
(Firma)

INFORMATIVA LAVORATORI DIPENDENTI

Lo scrivente Comune di Motta Sant'Anastasia Ente locale comunica che, per l'instaurazione e la gestione del rapporto di lavoro in corso, è titolare di dati Suoi e dei Suoi familiari(1) qualificati come dati personali ai sensi del Regolamento 2016/679 e della normativa nazionale in vigore.

FONTE DEI DATI PERSONALI

La raccolta dei dati personali viene effettuata da Comune di Motta Sant'Anastasia Ente locale registrando i dati:

- raccolti direttamente presso interessato, al momento del contatto iniziale o di successive comunicazioni
- forniti da terzi

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:

- Mista - elettronica e cartacea

I dati raccolti vengono utilizzati per le seguenti finalità:

- Amministrazione degli stranieri (rilascio di permessi, visti di riconoscimenti di titoli)
- Amministrazione della popolazione (anagrafe,registri dello stato civile)
- Attività politica
- Reclutamento, selezione, valutazione e monitoraggio del personale: concorsi interni
- Relazioni con il pubblico
- Riscossione imposte e tasse comunali

BASE GIURIDICA

Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Le basi giuridiche su cui si fonda il trattamento per categorie particolari di dati personali, secondo l'Art.9 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

La società tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati in Italia e trasferiti all'estero (3) esclusivamente per le finalità sopra specificate a:

- Associazioni ed enti locali;
- Clienti ed utenti;
- Diffusione al pubblico;
- Società e imprese;
- Soggetti che svolgono attività di archiviazione della documentazione;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati:

- Personale Aree aventi competenza sul personale
- Dedagroup spa, p.iva 01763870225 - Responsabile tecnico
- Halley Informatica , p.iva 00384350435 - Responsabile tecnico
- Cuscunà Giuseppe, c.f. CSCGPP65L07F781T - Medico competente

In relazione al rapporto di lavoro, l'azienda potrà trattare dati che la legge definisce "particolari" in quanto idonei a rilevare ad esempio:

a) lo stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);
b) l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale), l'adesione ad un partito politico o la titolarità di cariche pubbliche elettive (permessi od aspettativa), convinzioni religiose (festività religiose fruibili per legge);

I dati di natura particolare, concernenti lo stato di salute, che tratta il medico competente nell'espletamento dei compiti previsti dal D.Lgs. 81/08 e dalle altre disposizioni in materia di salute e sicurezza sui luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati presso il datore di lavoro esclusivamente dallo stesso medico quale Responsabile del trattamento del trattamento, per il quale la società chiede espresso consenso (4).

STRUTTURE INFORMATICHE

I dati saranno conservati presso le strutture informatiche del comune (o presso server siti in Italia o in UE) , con adeguate misure di sicurezza ai sensi delle linee guida pubblicate sulla G.U. n.79 del 04-04-2017 per le PA e non saranno accessibili a soggetti esterni che non siano stati preventivamente autorizzati.

DIRITTI DELL'INTERESSATO

Relativamente ai dati medesimi si potranno esercitare i diritti previsti dagli artt. 15 - "Diritto di accesso dell'interessato", 16 - "Diritto di rettifica", 17 - "Diritto alla cancellazione", 18 – "Diritto di limitazione al trattamento", 20 – "Diritto alla portabilità dei dati" del **Regolamento UE 2016/679** e normativa nazionale in vigore, nei limiti ed alle condizioni previste dall'art. 12 del Regolamento stesso.

PERIODO DI CONSERVAZIONE

Il periodo di conservazione dei dati è: I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.

Titolare del trattamento dei Suoi dati personali è Comune di Motta Sant'Anastasia Ente locale, p.iva 00575910872, c.f. 00575910872 nella persona di Carrà Anastasio sindaco pro- tempore

- Email: info@comune.mottasantanastasia.ct.it
- PEC: infopost@pec.comune.mottasantanastasia.ct.it

Lo scrivente Comune ha nominato quale DPO (Data Protection Officer) l'Ing. Antonio Corrente, p.iva 04675010872, nella persona di Corrente Antonio che può essere contattato al seguente indirizzo email: ing@antoniocorrente.it

Data Timbro e firma azienda

****

Il/I sottoscritto/i (1) in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data Firma

(1)

COGNOME	NOME	REL. DI PARENTELA	FIRMA
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

(1) Da inserire quando si trattano anche dati relativi ai familiari (ad esempio assegni per il nucleo familiare, permessi per assistenza ai familiari, ecc.). Il consenso deve essere sottoscritto dai familiari maggiorenni.
(2) Qualora il conferimento di alcuni dati non sia obbligatorio per legge o per contratto è necessario precisare la natura facoltativa, le finalità specifiche, nonché le conseguenze del mancato conferimento.
(3) E' opportuno quindi precisare se il trasferimento dei dati riguarda i paesi UE, o quelli extra UE.
(4) Da inserire nei casi in cui vi siano dipendenti sottoposti a sorveglianza sanitaria ai sensi della normativa vigente. Se il medico è qualificato quale titolare autonomo del trattamento si chiede il consenso per suo conto. In alternativa dovrà richiederlo direttamente il medico (secondo un apposito modello); in ulteriore alternativa potrebbe essere qualificato quale responsabile del trattamento (predisponendo in tal caso lo specifico atto di nomina riportato tra la modulistica).

Data

Firma

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI FORNITORI

I dati personali dell'utente sono utilizzati da Comune di Motta Sant'Anastasia, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

FONTE DEI DATI PERSONALI

La raccolta dei dati personali viene effettuata da Comune di Motta Sant'Anastasia Ente locale registrando i dati:

- raccolti direttamente presso interessato, al momento del contatto iniziale o di successive comunicazioni
- forniti da terzi

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:

- Mista - elettronica e cartacea

con le seguenti finalità:

- Amministrazione degli stranieri (rilascio di permessi, visti di riconoscimenti di titoli)
- Amministrazione della popolazione (anagrafe,registri dello stato civile)
- Attività politica
- Reclutamento, selezione, valutazione e monitoraggio del personale: concorsi interni
- Relazioni con il pubblico
- Riscossione imposte e tasse comunali

In particolare, per le finalità specificate di seguito i dati dell'utente saranno trattati SOLO su specifica accettazione del consenso:

- Relazioni con il pubblico

  ☐ accetta ☐ non accetta
- Consenso al trattamento di dati particolari:

  ☐ accetta ☐ non accetta

BASE GIURIDICA

Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Le basi giuridiche su cui si fonda il trattamento per categorie particolari di dati personali, secondo l'Art.9 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

La società tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:

- Associazioni ed enti locali;
- Clienti ed utenti;
- Diffusione al pubblico;

- Società e imprese;
- Soggetti che svolgono attività di archiviazione della documentazione;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati:

- Personale Area XXXXXXXXXXX
- Dedagroup spa, p.iva 01763870225 - Responsabile tecnico
- Halley Informatica , p.iva 00384350435 - Responsabile tecnico

STRUTTURE INFORMATICHE

I dati saranno conservati presso le strutture informatiche del comune (o presso server siti in Italia o in UE) , con adeguate misure di sicurezza ai sensi delle linee guida pubblicate sulla G.U. n.79 del 04-04-2017 per le PA e non saranno accessibili a soggetti esterni che non siano stati preventivamente autorizzati.

PERIODO DI CONSERVAZIONE

Il periodo di conservazione dei dati è: I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.

DIRITTI DELL'INTERESSATO

Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato - art. 15 del Regolamento 679/2016);
- conoscerne l'origine;
- riceverne comunicazione intelligibile;
- avere informazioni circa la logica, le modalità e le finalità del trattamento;
- richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione - artt. 16 e 17 del Regolamento 679/2016);
- diritto di limitazione o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
- diritto di revoca;
- diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
- nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
- il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato - art. 15 del Regolamento 679/2016).

Titolare del trattamento dei Suoi dati personali è Comune di Motta Sant'Anastasia Ente locale, p.iva 00575910872, c.f. 00575910872 nella persona di Carrà Anastasio sindaco pro- tempore

- Email: info@comune.mottasantanastasia.ct.it
- PEC: infopost@pec.comune.mottasantanastasia.ct.it

Lo scrivente Comune ha nominato quali DPO (Data Protection Officer)

- Dott. Ing. Antonio Corrente , p.iva 04675010872, che può essere contattato al seguente indirizzo email: ing@antoniocorrente.it.

****

Il/I sottoscritto/i (1) in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data Firma

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI AI CITTADINI

I dati personali dell'utente sono utilizzati da Comune di Motta Sant'Anastasia in qualità di Ente locale, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

FONTE DEI DATI PERSONALI

La raccolta dei dati personali viene effettuata da Comune di Motta Sant'Anastasia Ente locale registrando i dati:

- raccolti direttamente presso interessato, al momento del contatto iniziale o di successive comunicazioni
- forniti da terzi

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:

- Mista - elettronica e cartacea

con le seguenti finalità:

- Amministrazione degli stranieri (rilascio di permessi, visti di riconoscimenti di titoli)
- Amministrazione della popolazione (anagrafe, registri dello stato civile)
- Attività politica
- Reclutamento, selezione, valutazione e monitoraggio del personale: concorsi interni
- Relazioni con il pubblico
- Riscossione imposte e tasse comunali

In particolare, per le finalità specificate di seguito i dati dell'utente saranno trattati SOLO su specifica accettazione del consenso:

- Relazioni con il pubblico
  ☐ accetta ☐ non accetta
- Consenso al trattamento di dati particolari:
  ☐ accetta ☐ non accetta
- Consenso al trattamento di dati di minori (almeno 14 anni):
  ☐ accetta ☐ non accetta

BASE GIURIDICA

Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Le basi giuridiche su cui si fonda il trattamento per categorie particolari di dati personali, secondo l'Art.9 del Regolamento GDPR, sono:

- Legittimo interesse;
- Interesse pubblico;
- Salvaguardia degli interessi vitali;
- Legge;
- Consenso;

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.
La società tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:

- Associazioni ed enti locali;
- Clienti ed utenti;

- Diffusione al pubblico;
- Società e imprese;
- Soggetti che svolgono attività di archiviazione della documentazione;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati:

- Personale Area XXXXXXXXXX
- Dott. Ing. Antonio Corrente , p.iva 04675010872, nella persona di Corrente Antonio - Fornitore
- Dedagroup spa, p.iva 01763870225 - Responsabile tecnico
- Halley Informatica , p.iva 00384350435 - Responsabile tecnico
- Cuscunà Giuseppe, c.f. CSCGPP65L07F781T - Medico competente

CATEGORIE DI DATI PERSONALI

Secondo quanto esplicitato dall'articolo 14 del Regolamento GDPR, non essendo stati ottenuti i dati presso l'interessato, si riportano le categorie di dati personali oggetto di trattamento:

- Codice fiscale ed altri numeri di identificazione personale (carte sanitarie);
- Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.);
- Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro);
- Particolari (sensibili);
- Personali;

STRUTTURE INFORMATICHE

I dati saranno conservati presso le strutture informatiche del comune (o presso server siti in Italia o in UE) , con adeguate misure di sicurezza ai sensi delle linee guida pubblicate sulla G.U. n.79 del 04-04-2017 per le PA e non saranno accessibili a soggetti esterni che non siano stati preventivamente autorizzati.

PERIODO DI CONSERVAZIONE

I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.

DIRITTI DELL'INTERESSATO

Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato - art. 15 del Regolamento 679/2016);
- conoscerne l'origine;
- riceverne comunicazione intelligibile;
- avere informazioni circa la logica, le modalità e le finalità del trattamento;
- richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione - artt. 16 e 17 del Regolamento 679/2016);
- diritto di limitazione e/o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
- diritto di revoca;
- diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
- nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
- il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato - art. 15 del Regolamento 679/2016).

Titolare del trattamento dei Suoi dati personali è Comune di Motta Sant'Anastasia Ente locale, p.iva 00575910872, c.f. 00575910872, nella persona di Carrà Anastasio sindaco pro- tempore

- Email: info@comune.mottasantanastasia.ct.it
- PEC: infopost@pec.comune.mottasantanastasia.ct.it

Il comune ha nominato quali DPO (Data Protection Officer)

- Dott. Ing. Antonio Corrente , p.iva 04675010872, che può essere contattato al seguente indirizzo email: ing@antoniocorrente.it.

****

Il/I sottoscritto/i in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data _____ Firma _____

CONSENSO INFORMATO PER GENITORI/TUTORE LEGALE

Io sottoscritta (madre/tutore) _____
nata il ___/___/_____residente a_____ via/piazza _____ Tel._____ domicilio (se diverso dalla residenza) _____

Io sottoscritto (padre/tutore) _____
nato il ___/___/_____residente a_____ via/piazza _____ Tel. _____ domicilio (se diverso dalla residenza) _____

del minore _____ nato il ___/___/_____
residente a_____ via/piazza _____

dichiaro di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprimo il consenso al trattamento ed alla comunicazione dei dati personali di mio figlio/a, con particolare riguardo a quelli cosiddetti particolari, nei limiti, per le finalità e per la durata precisati nell'informativa fornitami con il presente documento.

_____	___/___/_____	_____
Nome per esteso del genitore/tutore legale	Data	Firma
_____	___/___/_____	_____
Nome per esteso del genitore/tutore legale	Data	Firma