Reg. Sett. 74 del 21-12-2023

Città di Pisticci
(Provincia di Matera)

DETERMINAZIONE N.	1548
Data di registrazione	21-12-2023

OGGETTO: INDIVIDUAZIONE DIPENDENTE INCARICATO AL TRATTAMENTO DEI DATI

IL CAPO SERVIZIO DEL
SERVIZIO LEGALE

PREMESSO che:

- il D.Lgs. 10 agosto 2018, n. 101, concernente "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, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), ha adeguato il D.Lgs. 30 giugno 2003 nr. 196 (Codice della Privacy) armonizzandolo alla normativa europea;
- l'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del D.Lgs. 196/2003 dispone che *"1) Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2) Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta."*

RICHIAMATO il Decreto Sindacale n. 11 del 10 ottobre 2023 con il quale sono stati designati i seguenti *"Delegati al trattamento dei dati":*

- il Segretario Generale del Comune di Pisticci, per le sue funzioni di Responsabile della prevenzione della corruzione e della trasparenza;
- dr. Giuseppina D'Aranno quale Dirigente Settore II e ad interim del Settore I
- ing. Rocco Salvatore Di Leo quale Dirigente del Settore III;
- ing. Salvatore Rocco Giannace quale Dirigente del Settore IV;
- avv. Patrizia Caruso quale Responsabile Avvocatura in posizione di Staff;
- Tenente dott.ssa Volpe Domenica quale Responsabile del Coordinamento e Controllo della Polizia Locale;

RILEVATO che il suddetto Decreto prevede, tra l'altro, che ciascun "*Delegato per la protezione dei dati*" è tenuto ad autorizzare il personale dipendente assegnato al Settore mediante atto individuale che specifichi il ruolo operativo assegnato e contenga le specifiche istruzioni rapportate alla funzione operativa, alle procedure, agli strumenti

autorizzati per ciascun incaricato e al relativo profilo applicativo, nonché vincoli l'operatore autorizzato all'obbligo di riservatezza

Dato Atto che:
- con deliberazione di Consiglio Comunale n. 10 in data 8 maggio 2023, esecutiva ai sensi di legge, è stata approvata la Nota di Aggiornamento al Documento Unico di Programmazione (DUP) relativo al periodo 2023/2025;
- con deliberazione di Consiglio Comunale n. 11 in data 8 maggio 2023, esecutiva ai sensi di legge, è stato approvato il Bilancio di Previsione finanziario 2023/2025 redatto in termini di competenza e di cassa secondo lo schema di cui al D. Lgs. n. 118/2011;
- con deliberazione di Giunta Comunale n. 81 in data 23/05/2023 esecutiva è stato approvato il PIANO ESECUTIVO DI GESTIONE 2023/2025;

Visto il D.Lgs. 30/03/2001, n. 165 e s.m.i.;

Visto l'art. 15 del D.Lgs. n. 33/2013, che disciplina gli obblighi di pubblicazione concernenti i titolari di incarichi di collaborazione o consulenza;

Visto il D.Lgs. n. 267/2000 e s.m.i.;

Richiamati l'art. 107 del D.Lgs 18/08/2000, n. 267, e l'art. 4 del D.Lgs. 30/03/2001, n. 165, i quali, in attuazione del principio della distinzione tra indirizzo e controllo, da un lato, e attuazione e gestione, dall'altro, prevedono che:

- *gli organi di governo esercitano le funzioni di indirizzo politico-amministrativo, ovvero definiscono gli obiettivi e i programmi da attuare, adottano gli atti rientranti nello svolgimento di tali funzioni e verificano la rispondenza dei risultati dell'attività amministrativa e della gestione agli indirizzi impartiti;*
- *ai dirigenti spettano i compiti di attuazione degli obiettivi e dei programmi definiti con gli atti di indirizzo. Ad essi è attribuita la responsabilità esclusiva dell'attività amministrativa, della gestione e dei relativi risultati in relazione agli obiettivi dell'ente;*

Attesa la propria competenza ai sensi del combinato disposto degli articoli 107, 2° e 3° comma, e 109, 2° comma, del D.lgs. 18.8.2000, n. 267, ed accertato che il provvedimento è formulato in conformità a quanto previsto in materia dalla vigente normativa, nonché nel rispetto degli atti che costituiscono il presupposto delle procedure;

Dato atto che, ai sensi dell'art. 147 bis del D.Lgs. n. 267/2000 e s.m.i., la regolarità tecnica del presente provvedimento in ordine alla regolarità, legittimità e correttezza dell'azione amministrativa è resa unitamente alla sottoscrizione del presente provvedimento;

D E T E R M I N A

Di RICHIAMARE tutto quanto in premessa, quale parte integrante e sostanziale del presente provvedimento;

DI NOMINARE il dipendente ALO' Maria, quale incaricato autorizzato al trattamento delle seguenti tipologie di dati strettamente connesse alla attività lavorativa e relativi all'Ufficio Legale ed in particolare:

- dati personali ed identificativi (tutte le informazioni che permettano l'identificazione del soggetto cui si riferiscono es. dati anagrafici, recapiti telefonici, fotografie, codici identificativi, ecc.);
- dati Particolari (origine razziale o etnica, appartenenza sindacale, dati relativi alla salute);
- dati giudiziari.

DI DARE ATTO CHE per *trattamento* è da considerarsi qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.
Nello specifico, ferma restando la preventiva configurazione degli strumenti messi a disposizione dell'Ente, quale incaricato, avrà accesso agli strumenti e potrà trattare i dati, elencati in maniera non esaustiva, contenuti in:

- *Posta elettronica*
- *Navigazione Internet*
- *Pacchetto Office Microsoft*
- *Accesso alle cartelle elettroniche presenti su file server*
- *Accesso alla cartella elettronica assegnata*
- *Accesso alle stampanti*
- *Area Intranet dell'Ente*
- *DB – Gestione contratti avvocati esterni all'Ente*
- *DB Dati fornitori*
- *Archivio cartaceo del suo ufficio*
- *File contenente dati personali*
- *File contenente dati particolari*
- *File e software contenente dati giudiziari;*

DI DARE ATTO, altresì, che:

- Senza preventiva autorizzazione non è permesso realizzare nuove ed autonome banche dati e perseguire finalità differenti rispetto a quelle definite.

- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dal titolare del trattamento e per quanto concerne la sua mansione devono essere trattati solo i dati strettamente necessari per ottemperare al rapporto lavorativo.

- L'eventuale raccolta di dati, come ogni trattamento, dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati dall'Ente e messi a disposizione delle persone incaricate.

- È necessario prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi attenendosi alle istruzioni contenute nella presente nomina.

- In relazione ai dati e alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, ogni ipotesi di comunicazione o di diffusione dei dati a soggetti esterni dovrà essere preventivamente autorizzata di volta in volta; è pertanto vietato diffondere o comunicare dati di propria iniziativa.

- In caso di dubbi sulla gestione dei trattamenti connessi alla propria attività professionale, l'incaricato dovrà rivolgersi al titolare o al responsabile qualora nominato prima di effettuare qualunque trattamento.

- L'incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, modifica non autorizzata, predisposte o che saranno successivamente implementate.

DI STABILIRE, inoltre, che:

- ***Per i Trattamenti Cartacei:***

- In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrà trattare ed accedere agli archivi relativi alle banche dati strettamente connessi alla propria mansione e sopra rammentati.
- Dovrà provvedere a chiudere gli archivi contenenti dati alla fine della giornata lavorativa.
- I documenti (o copia degli stessi) non possono essere, senza specifica autorizzazione, asportati dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati.
- Durante l'utilizzazione i documenti, ed i fascicoli cartacei, non devono essere lasciati incustoditi;
- In caso di assenza temporanea durante l'utilizzo i documenti vanno riposti nei cassetti o armadietti a sua disposizione o chiusi negli uffici per evitare che possano essere effettuati trattamenti da soggetti non autorizzati.
- Per l'accesso ai dati al di fuori del normale orario di lavoro dovrà essere chiesta specifica autorizzazione.

- ***Per i Trattamenti tramite sistemi informatici:***

- All'incaricato al trattamento dati è assegnato un codice di identificazione personale ed un'utenza opportunamente configurata per poter permettere il trattamento esclusivo dei dati di propria pertinenza: è vietato modificare le configurazioni preimpostate senza preventiva autorizzazione espressa.
- L'accesso ai sistemi dell'Ente è consentito esclusivamente tramite le credenziali assegnate al singolo soggetto autorizzato al trattamento.
- Potranno essere predisposte ulteriori misure per l'accesso ai sistemi ed alle banche dati dell'Ente, che in ogni caso saranno definiti di default per garantire l'accesso profilato per singolo autorizzato; quanto indicato in tema di divieti di modifiche delle configurazioni, di segretezza degli strumenti/processi di accesso ai sistemi si deve considerare esteso ad ogni strumento/modalità/presidio.
- La postazione informatica, come pure eventuali device (tablet, sistemi portatili, cellulari), non va lasciata incustodita ed eventuali supporti esterni di memorizzazione utilizzati (nb utilizzabili solo a seguito di autorizzazione espressa) vanno riposti in cassetti o armadietti o qualora possibile protetti da password, e dovranno essere adottate le ulteriori misure che saranno comunicate a seguito dell'autorizzazione all'utilizzo di tali strumenti.
- I supporti non più utilizzati possono essere eliminati solo a seguito di autorizzazione e solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili. Anche in questo caso sarà necessario seguire le istruzioni di volta in volta fornite.
- È necessario collaborare proattivamente nel verificare il funzionamento e l'aggiornamento corretto degli strumenti affidati. In caso di malfunzionamento o dubbi dovrà essere prontamente data comunicazione.
- L'incaricato/autorizzato non può installare e utilizzare programmi o strumenti non autorizzati.
- Gli strumenti informatici e telematici messi a disposizione (a seconda dei casi: computer; laptop, smartphone, software; navigazione su Internet, e-mail etc etc) costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate. Si ricorda che sono, quindi, vietati gli usi personali, quali ad esempio la conservazione di documenti personali non inerenti l'attività lavorativa, l'uso delle mail o di qualunque sistema per scopi non legati allo svolgimento della mansione (si rinvia per indicazioni ulteriori al regolamento specifico prodotto dagli scriventi).
- La password dovrà essere modificata ogni 90 giorni.
- La password dovrà essere composta da almeno 10 caratteri e non potrà essere riutilizzata in momenti successivi.
- Le variazioni della password sono disposte autonomamente secondo le procedure preimpostate che possono prevedere anche sistemi informatici che impongono la modifica della credenziale alle scadenze prefissate oppure tramite la richiesta di personale appositamente incaricato; è in ogni caso obbligatoria la modifica da parte dell'utente.

- La propria password e il nome utente assegnato non dovranno essere rivelati a nessuno e per alcun motivo, a meno di nomina di un fiduciario ed/o un custode password, che conserverà in busta chiusa sigillata la credenziale.
- Il Titolare del Trattamento si riserva, in sua assenza e nei soli casi di estrema necessità di accesso per poter ottemperare alle attività lavorative, di utilizzare la password consegnata al custode Password o di operare tramite Amministratore di Sistema o il fiduciario, se nominato. In tali casi si redigerà apposito verbale, verrà prontamente informato/a e l'utenza, a seguito dell'uso necessario, sarà temporaneamente bloccata e non più utilizzata sino al suo rientro a seguito del quale dovrà immediatamente modificare le proprie credenziali di accesso.
- Non deve essere conservato alcun appunto con la password per evitare che altri ne vengano, anche accidentalmente, a conoscenza. Nel caso di sospetto che altri siano a conoscenza della propria password si dovrà informare il titolare e modificare immediatamente le proprie credenziali.
- Le banche dati a cui si ha accesso, ed i dati in esse contenuti, devono essere utilizzate per il solo scopo per cui sono state create. Si devono quindi effettuare esclusivamente le operazioni di trattamento per i quali si è autorizzati per lo svolgimento delle proprie mansioni. Qualora avesse dubbi su come procedere o su quali trattamenti effettuare dovrà darne immediata comunicazione al titolare del trattamento ed attendere istruzioni in merito.
- Le banche dati ed i dati ivi contenuti non devono essere asportati né inviati all'esterno. Eventuali comunicazioni di informazioni a terzi possono essere ammesse solo ove necessarie alla propria attività lavorativa e a seguito di autorizzazione e di istruzioni conseguenti. Si ricorda che i dati devono essere a disposizione unicamente delle persone che hanno diritto ad accedere alle stesse, previa autorizzazione del Responsabile del Trattamento o del Titolare; ne consegue che il personale non autorizzato non deve avere accesso, neppure in maniera occasionale, ai dati e alle banche dati presenti nella rete dell'Ente o ai dati e alle banche dati cartacee.
- In caso di cessazione dell'utilizzo di una banca dati deve essere data comunicazione ed operare secondo le procedure che saranno fornite;
- Qualora il proprio computer non venga temporaneamente utilizzato, lo screensaver è impostato per bloccarsi automaticamente dopo un tempo predeterminato. Tale configurazione sarà impostata di default. L'incaricato/autorizzato dovrà verificare che sia sempre in essere e dare comunicazione qualora ci fossero problematiche o tale funzione non funzionasse correttamente. Inoltre, in caso di allontanamento dalla postazione di lavoro, il blocco dovrà essere predisposto direttamente dallo stesso in modo da evitare che lo strumento possa essere, anche se per breve periodo, a disposizione di terzi.
- È vietato l'utilizzo di cd rom, chiavette usb, hard disk e di altri supporti o di programmi che non siano stati forniti dal titolare e/o come pure è vietato installare modem o altri apparecchi non autorizzati dal titolare o dal responsabile.
- È vietata la conservazione di file o qualunque documento (audio video mail cartaceo) non inerenti l'attività lavorativa.
- E' vietato lasciare files contenenti dati in locale, essendo tenuto salvarne copia sui server dell'ente sottoposti a back up.

DI DARE ATTO CHE il presente provvedimento non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente e che acquisterà efficacia immediata dal momento della pubblicazione all'Albo pretorio comunale;

DI DARE ATTO CHE relativamente al presente provvedimento non sussistono situazioni di conflitto di interesse, ai sensi dell'art. 6 bis della legge 241/90, nei confronti della sottoscritta, neanche potenziale;

DI ADEMPIERE agli obblighi di pubblicazione del presente provvedimento nella Sezione amministrazione trasparente, prevista dal D.Lgs. n.33/2013;

DI DARE ATTO CHE la pubblicazione avverrà nel rispetto dei principi sanciti dal Regolamento (UE) n.679/16, seguito del quale è stato emanato il D.Lgs.10/08/2018 n.101, di adeguamento della normativa nazionale ed in ogni caso nel rispetto dei principi "di necessità", "di pertinenza e non eccedenza".

Il Responsabile Del Procedimento
Caruso Patrizia

Il Capo Servizio
Caruso Patrizia

CERTIFICATO DI PUBBLICAZIONE

In pubblicazione all'Albo Pretorio on-line al n. 3018 per gg. 15 Dal 21-12-2023

IL

Documento firmato digitalmente ai sensi del TU n. 445/00, dell'art. 20 del D.lgs. 82/2005 e norme collegate. Tale documento informatico è memorizzato digitalmente sulla banca dati dell'Ente.

Copia conforme all'originale informatico, per uso amministrativo.

Pisticci, 21/12/2023

_____