



COMUNE DI FIUMEDINISI

CITTÀ METROPOLITANA DI MESSINA

IL LAVORO AGILE NEL NUOVO CCNL 16/11/2022

Il nuovo CCNL Comparto Funzioni Locali triennio 2019-2021, sottoscritto in data 16/11/2022, si incarica di dare forma contrattuale all'istituto, e ne conferma le principali caratteristiche:

- prestazioni senza vincoli di orario o luogo di lavoro, senza una postazione fissa predefinita ma nel rispetto di misure di sicurezza per il lavoratore e per i dati trattati;
- organizzazione del lavoro per fasi, cicli e obiettivi;
- necessità di un Regolamento di Ente e dell'accordo Individuale;
- parità di diritti e di opportunità lavorative.

ALLEGATO – MODELLO RICHIESTA LAVORO AGILE

Al Responsabile _____.

Al Segretario Comunale
SEDE

MANIFESTAZIONE DI INTERESSE ALL'AVVIO DI UN PROGETTO INDIVIDUALE DI LAVORO AGILE

Il/La sottoscritto/a _____ nato/a _____ prov. _____ il _____ residente in _____ prov. _____ via _____ CAP _____ in servizio presso Codesto Ufficio con la qualifica di _____ Tel. uff. _____ Email _____

MANIFESTA IL PROPRIO INTERESSE

all'avvio di un progetto individuale di lavoro agile per lo svolgimento della seguente attività:

.....

DICHIARA (*barrare opzione desiderata*)

di necessitare per lo svolgimento della prestazione lavorativa da remoto, della seguente strumentazione tecnologica fornita dall'Amministrazione:

di non necessitare di alcuna strumentazione fornita dall'Amministrazione essendo in possesso della seguente strumentazione tecnologica:

DICHIARA

di aver preso visione della disciplina approvata con la deliberazione di Giunta comunale succitata e di accettare tutte le disposizioni ivi previste;
di aver preso visione dell'Informativa sulla salute e sicurezza nel lavoro agile di cui all'allegato _____ della citata deliberazione.

Individua il Domicilio per lo svolgimento della prestazione lavorativa in modalità agile il seguente luogo (*barrare una casella ed indicare l'indirizzo*):

- Residenza _____
- Domicilio _____
- Altro luogo (da specificare) _____

Parte eventuale → Dichiaro inoltre di trovarmi in una delle condizioni di precedenza per il L.A., nella specie _____ (*INDICARE FATTISPECIE*)

Si allegano alla presente richiesta:

1. copia fotostatica del documento di identità
2. _____

Si autorizza il trattamento dei dati personali ai sensi del GDPR (Reg. UE n. 679/2016).

_____, li _____

In fede

ACCORDO INDIVIDUALE

L'accordo può essere stipulato a termine o a tempo indeterminato. La scadenza dell'accordo a tempo determinato può essere prorogata previa richiesta scritta del dipendente al proprio Responsabile di riferimento; il Responsabile comunicherà al Servizio Personale l'avvenuta proroga. Il Responsabile di riferimento respinge o approva la richiesta del dipendente eventualmente proponendo modifiche. L'accordo individuale, sottoscritto entro 30 giorni dalla presentazione dell'istanza tra il dipendente ed il Responsabile del Servizio di riferimento, deve redigersi inderogabilmente sulla base del modello predisposto dall'Amministrazione.

Copia dell'accordo individuale sottoscritto è inviata dal dipendente al Servizio Personale per le dovute comunicazioni di cui all'art. 23 della L. 81/2017. L'accordo costituisce un addendum al contratto individuale di lavoro.

L'accordo individuale di cui all'art. 18, comma 1, della legge 22 maggio 2017, n. 81, deve definire, almeno:

- 1) gli specifici obiettivi della prestazione resa in modalità agile;
- 2) le modalità e i tempi di esecuzione della prestazione e della disconnessione del lavoratore dagli apparati di lavoro, nonché eventuali fasce di contattabilità;
- 3) le modalità e i criteri di misurazione della prestazione medesima, anche ai fini del proseguimento della modalità della prestazione lavorativa in modalità agile.

Durante la fase di svolgimento della prestazione in lavoro agile è possibile, previa intesa tra le parti, modificare le condizioni previste nell'accordo individuale, sia per motivate esigenze espresse dal lavoratore, sia per necessità organizzative e/o gestionali dell'Amministrazione.

In caso di eventuali modifiche riguardanti il profilo professionale del dipendente o dell'attività svolta dal medesimo, la prosecuzione della prestazione in L.A. è condizionata alla sottoscrizione di un nuovo accordo individuale. L'accordo individuale e le sue modificazioni sono soggetti, a cura dell'Amministrazione, alle comunicazioni di cui all'articolo 9-bis del decreto-legge 1° ottobre 1996, n. 510, convertito, con modificazioni, dalla legge 28 novembre 1996, n. 608, e successive modificazioni.

ACCORDO INDIVIDUALE PER LA PRESTAZIONE IN LAVORO AGILE

TRA

_____ nato/a a _____ il _____, in qualità di Responsabile del Servizio

E

il/ la dipendente _____ nato/a a _____ il _____, con profilo di

Vista l'istanza del lavoratore presentata con nota prot. n. _____ del _____;

Visto il vigente Piano Operativo per il Lavoro Agile (POLA);

Visto il Decreto del Ministro per la pubblica amministrazione dell'8/10/2021;

Visto il Capo I del titolo VI del CCNL Funzioni Locali del 16/11/2022;

SI CONVIENE QUANTO SEGUE

che il/la dipendente, come meglio sopra identificato/a, è autorizzato/a a svolgere la prestazione lavorativa in modalità agile nei termini ed alle condizioni di seguito indicate ed in conformità alle prescrizioni stabilite nella disciplina sopra richiamata:

attività da svolgersi in modalità agile (*fornire un'indicazione dettagliata delle attività e dei procedimenti da svolgersi in modalità agile*): _____

obiettivi della prestazione resa in modalità agile (*descrivere i risultati ed i comportamenti attesi durante il periodo di lavoro agile*): _____

data di avvio prestazione in modalità lavoro agile: _____

data di fine della prestazione lavoro agile: _____

giorno/i settimanale/i di svolgimento della prestazione in modalità agile: _____

ai fini dello svolgimento dell'attività lavorativa in modalità agile, si prevede l'utilizzo della seguente dotazione tecnologica e strumentale (*connessione internet, VPN, cellulare, personal computer portatile, ecc.*): _____, di proprietà del dipendente e/o dell'amministrazione (*specificare*).

La strumentazione sopra indicata è valutata come idonea alle esigenze dell'attività lavorativa, nel rispetto delle norme di sicurezza vigenti.

(*solo in caso di dotazione tecnologica fornita dall'Amministrazione, aggiungere*: ed è fornita al lavoratore in comodato d'uso, secondo la disciplina di cui all'articolo 1803 e ss. del Codice Civile).

Le spese riguardanti i consumi elettrici, nonché il costo della connessione dati sono a carico del lavoratore. Il Comune adotta le soluzioni tecnologiche necessarie a consentire al dipendente l'accesso da remoto alla postazione di lavoro e/o ai sistemi applicativi necessari allo svolgimento della prestazione tramite il dispositivo ad uso del lavoratore;

fascia di contattabilità obbligatoria del dipendente: mattina dalle _____ alle _____ e, in caso di giornata con rientro pomeridiano, dalle _____ alle _____.

ALLEGATI ALL'ACCORDO INDIVIDUALE

ISTRUZIONI DI LAVORO DA OSSERVARE DURANTE LE SESSIONI REMOTE DA PARTE DEGLI OPERATORI DELL'ORGANIZZAZIONE ATTRAVERSO L'UTILIZZO DI DISPOSITIVI ELETTRONICI PERSONALI O, SE FORNITI DALL'ORGANIZZAZIONE, DI DISPOSITIVI PERSONALIZZABILI

Viste le prescrizioni di cui all'art. 12 del D. Lgs. 82/2005, che disciplinano le norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa, si autorizza _____ al trattamento dei dati personali secondo le modalità specificate nel presente documento, in cui sono indicate le specifiche istruzioni da seguire per garantire adeguate misure tecniche ed organizzative per la sicurezza dei dati durante le sessioni di lavoro remoto.

Istruzioni specifiche sul trattamento dei dati

Si rammenta quanto disposto dall'art. 5 del Regolamento UE 2016/679. I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Inoltre si richiama particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati durante le sessioni remote:

- cautela in qualsiasi trattamento effettuato su dati personali;
- trattamento esclusivo dei dati necessari all'attività lavorativa, astenendosi dal trattare i dati eccedenti le finalità;
- attenzione nel garantire la confidenzialità della documentazione trattata e la messa in sicurezza dei supporti messi in dotazione dall'ente.

Inoltre occorrerà osservare scrupolosamente tutte le misure di sicurezza già in atto e quelle che saranno successivamente adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti.

Infine si fa presente che tutte le disposizioni di futura emanazione correttive od integrative della normativa attualmente vigente in materia di protezione dei dati personali devono essere

scrupolosamente osservate.
Le presenti indicazioni sono tassative.

UTILIZZO DEI SUPPORTI E DEGLI STRUMENTI DI LAVORO

Chiavi: [qualora sia prevista anche la specifica dotazione di chiavi di accesso fisico]

- Qualora si disponga di chiavi di accesso agli uffici e alle sedi, è obbligatorio custodirle in sicurezza e segnalare immediatamente eventuali casi di furto o smarrimento.
- I dati trattati devono essere custoditi in luoghi non accessibili a soggetti non autorizzati. La custodia in sicurezza può essere garantita attraverso la chiusura a chiave di armadi e/o interi locali.

Documenti e supporti, analogici e digitali:

- Durante l'attività lavorativa, è consentito solamente trattare soltanto i dati necessari, astenendosi dal trattare dati eccedenti le finalità.
- Verificare sempre che la documentazione cartacea presa in carico venga adeguatamente inventariata al momento dell'uscita dalla sede dell'organizzazione, così come venga adeguatamente tracciata la sua restituzione.
- In caso di consultazione di documenti cartacei in luoghi in cui sono presenti altri soggetti, prestare sempre attenzione che non possano essere lette, neanche accidentalmente, le informazioni ivi contenute. Prestare sempre attenzione a non mostrare in chiaro eventuali nomi presenti su documenti o fascicoli che li contengano.
- Non lasciare incustoditi in luoghi pubblici (bar, parcheggi, ecc) documenti cartacei e supporti di memorizzazione digitale.

Strumenti di elaborazione:

- Eventuali postazioni di lavoro portatili messe a disposizione dal titolare per lo svolgimento delle attività lavorative vanno sempre presidiate e non vanno mai lasciate incustodite in luoghi pubblici. [qualora sia prevista la messa a disposizione di strumenti di proprietà dell'ente]
- Non lasciare incustoditi o accessibili a terzi non autorizzati la postazione di lavoro e gli strumenti elettronici mentre è in corso una sessione di lavoro.
- Accertarsi di non rendere conoscibili a soggetti indiscriminati i dati trattati, prestando attenzione che nessuno possa vedere le informazioni gestite attraverso gli strumenti di elaborazione, specie se le sessioni lavorative sono effettuate in luoghi pubblici.
- Qualora un tecnico richieda di collegarsi alla postazione di lavoro tramite strumenti di controllo remoto, è indispensabile
 - o verificare l'identità dell'operatore remoto (tramite conoscenza diretta o comunicazione preventiva)
 - o controllare se è autorizzato allo svolgimento dell'intervento (tramite preventiva apertura di ticket, autorizzazione)
 - o presidiare la postazione durante l'intervento, a meno che non sia stato concordato diversamente.

Credenziali di accesso:

- Non utilizzare password semplici, brevi e/o riconducibili alla propria realtà personale (data di nascita, nomi di parenti, ecc).
- Per sistemi diversi devono essere utilizzate credenziali diverse, al fine di mitigare i rischi legati al password reuse.
- Le credenziali personali di accesso ai sistemi devono essere custodite in sicurezza (senza lasciarle scritte in prossimità della postazione di lavoro).
- Prestare sempre attenzione che altri soggetti non siano in grado di vedere le password digitate.

- Non condividere credenziali di accesso con colleghi, è fondamentale che gli utenti utilizzino credenziali assegnate in maniera univoca.

Posta elettronica e internet:

- Durante la navigazione su internet e la fruizione di servizi on line, non utilizzare le stesse credenziali di accesso per ambiti professionali e per contesti di carattere privato.
- Limitare al minimo la navigazione internet contemporanea per finalità private e professionali, utilizzando finestre o browser differenti per i due ambiti.
- Per la comunicazione telematica di dati e documenti di carattere professionale utilizzare esclusivamente strumenti ufficiali messi a disposizione dall'organizzazione. Astenersi tassativamente dall'utilizzo di sistemi in rete (cloud) di carattere privato per veicolare informazioni di tipo lavorativo.
- Non utilizzare le stesse password per caselle di posta private e per caselle di lavoro.
- Non utilizzare lo stesso strumento di consultazione delle caselle di posta (browser, client di posta) per le caselle private e per le caselle di lavoro.
- Non inoltrare dati e documenti di lavoro su caselle private. Qualora incidentalmente delle informazioni di carattere professionale siano state veicolate su caselle di posta private è necessario rimuoverle il prima possibile, e comunque immediatamente dopo il loro utilizzo in ambito professionale.

Sicurezza dei contesti domestici utilizzati per attività lavorativa:

- I dispositivi personali messi a disposizione dall'utente devono essere equipaggiati almeno con sistemi antivirus, oltre che di eventuali ulteriori sistemi di sicurezza messi a disposizione dall'organizzazione; devono inoltre essere provvisti di tutti i più recenti aggiornamenti sicurezza del sistema operativo del dispositivo utilizzato.
- È necessario separare tempi e contesti professionali da quelli della vita privata, limitando al minimo la convivenza di questi aspetti al fine di evitare commistioni che potrebbero comportare rischi alla riservatezza delle informazioni trattate in ambito lavorativo.
- Le postazioni di lavoro private tramite le quali si trattano dei dati per conto dell'organizzazione devono essere protette con password di accesso dedicate all'attività lavorativa; le credenziali dedicate alle attività lavorative non devono essere condivise con altri soggetti conviventi o congiunti.
- Lo scaricamento di dati e documenti correlati all'ambito lavorativo sulla postazione di lavoro locale deve attenersi al principio di necessità, limitandosi al minimo indispensabile. È importante ricordare che l'utilizzo in locale di documenti comporta lo scaricamento di files in cartelle specifiche (es. cartelle "Temp" dedicate a particolari programmi o cartella "download"), per cui occorre verificare l'eventuale persistenza di copie di lavoro.
- In caso di scaricamento di dati e documenti per attività lavorative sulla postazione di lavoro privata, questi devono essere localizzati in ambienti informatici protetti con password e devono persistere sulle postazioni per il tempo minimo necessario a perseguire le finalità di carattere professionale, dopo di che vanno messi in sicurezza nella rete dell'organizzazione e cancellati dalla postazione di lavoro.
- Il salvataggio di dati e documenti correlati all'ambito professionale può essere effettuato solo su supporti dedicati all'utilizzo esclusivamente lavorativo; non è consentito l'utilizzo promiscuo di supporti di memorizzazione per dati di carattere privato e di carattere professionale.

Interazione con le strutture preposte alla gestione ICT dell'organizzazione

- È necessario attenersi a tutte le istruzioni contenute nel presente documento e alle ulteriori istruzioni di carattere operativo e tecnico che l'organizzazione potrebbe fornire.

Rapporto con soggetti terzi

- Prima di rilasciare documenti, dati o credenziali a soggetti terzi, verificare l'identità dei destinatari e la presenza di adeguate autorizzazioni al rilascio.
- Comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare.
- In caso di richieste di informazioni o documenti confrontarsi prontamente con il referente del Titolare sul da farsi.

Incidenti di sicurezza

Qualora si riscontri un incidente di sicurezza sulle risorse informative o sugli strumenti dati in dotazione dal Titolare, che possa o meno sfociare in una violazione da notificare all'autorità Garante della Privacy, è necessario comunicarlo immediatamente al referente del Titolare, al fine di allestire prontamente adeguate misure di mitigazione del danno.

Interventi di emergenza che necessitino l'utilizzo di credenziali dell'incaricato

In caso di necessità che renda indispensabile e indifferibile intervenire con le credenziali assegnate, per esclusive necessità di garantire la continuità dei servizi e/o la sicurezza dei dati, potrà essere consentito ad un soggetto specificamente designato l'accesso ai dati ed agli strumenti informatici, tramite modifica delle password dell'utente. Non appena possibile il personale espressamente designato dal Titolare provvederà ad informare l'assegnatario delle credenziali dell'avvenuta procedura. Al suo rientro questi dovrà obbligatoriamente provvedere ad impostare nuove password di accesso.

luogo

data

Per presa visione

INFORMATIVA AI SENSI REGOLAMENTO UE 2016/679 PER IL TRATTAMENTO DEI DATI DI CARATTERE TECNICO/ORGANIZZATIVO EFFETTUATO NELL'AMBITO DELLE ATTIVITÀ LAVORATIVE SVOLTE DA REMOTO (ART. 12 D.LGS. 82/2005)

La informiamo che i dati raccolti saranno trattati ai sensi della normativa vigente in tema di protezione dei dati personali. I dati trattati sono le credenziali di accesso al sistema da remoto (che non saranno comunque conosciute da altri soggetti, se non eventualmente nella fase di primo rilascio) [qualora vengano fornite specifiche credenziali di accesso] e il tracciamento dei tempi di sessione da remoto al sistema informativo del Titolare, limitandosi alla memorizzazione degli orari di inizio e di fine sessione. Sono inoltre tracciate le informazioni di presa in carico e di scarico di documenti e strumenti di lavoro da parte del dipendente, previste per lo svolgimento della prestazione di "lavoro agile".

Il trattamento viene effettuato con finalità correlate alla gestione dei dati nel contesto dell'iniziativa "lavoro agile", come previsto dalla legge 81/2017 in combinato con il DPCM 4 marzo 2020 oltre che dall'art. 12 del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale), ai sensi dall'art. 6 par. 1 lett. b) del Regolamento UE 679/2016.

I Suoi dati potranno essere trattati da soggetti privati e pubblici per attività strumentali alle finalità indicate, di cui l'organizzazione si avvarrà come responsabili del trattamento. Potranno essere inoltre comunicati a soggetti pubblici per l'osservanza di obblighi di legge, sempre nel rispetto della normativa vigente in tema di protezione dei dati personali.

Non è previsto il trasferimento di dati in un paese terzo, a meno che il trattamento non sia tutelato da specifiche clausole di salvaguardia.

Le comunichiamo inoltre che il conferimento dei dati è necessario per l'osservanza degli adempimenti di legge e l'adozione di adeguate misure tecniche e organizzative volte ad assicurare il trattamento dei dati in sicurezza, e che qualora non verranno acquisite tali informazioni non sarà possibile ottemperare agli obblighi di legge.

I dati saranno conservati per il tempo necessario a perseguire le finalità indicate e nel rispetto degli obblighi di legge previsti dalle normative.

Potrà far valere, in qualsiasi momento e ove possibile, i Suoi diritti, in particolare con riferimento al diritto di accesso ai Suoi dati personali, nonché al diritto di ottenerne la rettifica o la limitazione, l'aggiornamento e la cancellazione, oltre che al diritto di opposizione al trattamento, salvo vi sia un motivo legittimo del Titolare del trattamento che prevalga sugli interessi dell'interessato, ovvero per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Titolare non adotta alcun processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del Regolamento UE n. 679/2016.

Ha diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali qualora ne ravvisi la necessità.

Potrà esercitare i Suoi diritti rivolgendosi al Titolare o al Responsabile della protezione dei dati, reperibili ai contatti di seguito indicati.

Il Titolare del trattamento dei dati è il comune di Fiumedinisi che Lei potrà contattare ai seguenti riferimenti: Telefono: 0942/771001 – E-mail: protocollo@comune.fiumedinisi.me.it
Indirizzo PEC: comune.fiumedinisi@legalmail.it

luogo

data

Firma per esteso e leggibile per presa visione
