ALLEGATO A
Accordo individuale per la prestazione in lavoro agile

La/Il sottoscritta/o_____ , dipendente del Comune di _____,
Area/Servizio _____, in qualità di _____, a

tempo (indeterminato/determinato; pieno/parziale) _____
e

La/il sottoscritta/o _____ Dirigente/Responsabile dell'Area/Servizio
_____ ;

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

Visto il vigente Piano Operativo per il Lavoro Agile (POLA) approvato con D.G.C. n. _____;

Vista la direttiva del 29 dicembre 2023 del Ministro per la pubblica amministrazione;

Visto il CCNL vigente del 16/11/2022;

CONVENGONO 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 _____.

Trattamento giuridico ed economico, disposizioni organizzative, obblighi di riservatezza e di sicurezza sul
lavoro:

1 - Lo svolgimento della modalità agile della prestazione lavorativa da parte del dipendente non incide sulla natura giuridica del rapporto di lavoro subordinato in atto, che resta regolato dalle norme legislative e dai contratti collettivi nazionali e integrativi.

2 - La prestazione lavorativa resa con la modalità agile è integralmente considerata come servizio pari a quello ordinariamente reso presso le sedi abituali ed è utile ai fini della progressione in carriera, del computo dell'anzianità di servizio, nonché dell'applicazione degli istituti relativi al trattamento economico accessorio.

3 - La verifica circa il completamento delle attività assegnate è effettuata dal responsabile del servizio secondo modalità flessibili scelte discrezionalmente dallo stesso in funzione delle attività da eseguire in lavoro agile.

4 - La modalità di lavoro agile si svolge senza precisi vincoli di orario, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale contrattualmente previsti.

5 - Il lavoratore deve rispettare il riposo giornaliero pari a 11 ore consecutive, nel quale il lavoratore non può
erogare alcuna prestazione lavorativa (fascia di inoperabilità - disconnessione), come previsto dalla normativa vigente. Ha inoltre il diritto-dovere di astenersi dalla prestazione lavorativa nella fascia di lavoro notturno individuata dalla vigente normativa (dalle ore 22.00 alle ore 6.00).

6 - Al lavoratore è riconosciuto altresì il diritto alla disconnessione in occasione della pausa pranzo in una fascia oraria a sua scelta. Inoltre, come previsto dalla vigente normativa in materia di salute e sicurezza sui luoghi di lavoro, i lavoratori video-terminalisti sono tenuti ad effettuare una pausa di 15 minuti ogni 120 minuti di lavoro.

7 - Il lavoro agile non va effettuato durante il riposo settimanale, le giornate festive e di assenza per ferie, riposo, malattia, infortunio, aspettativa o altro istituto.

8 - Per effetto della distribuzione flessibile del tempo di lavoro, nelle giornate di lavoro agile non è riconosciuto il trattamento di trasferta, lavoro disagiato, lavoro svolto in condizioni di rischio e non sono configurabili prestazioni straordinarie, notturne o festive né permessi brevi, recupero ore straordinarie o riposi compensativi. Il lavoratore può richiedere, ove ne ricorrano i relativi presupposti, la fruizione dei permessi
orari previsti dai contratti collettivi o dalle norme di legge quali, a titolo esemplificativo, i permessi per particolari motivi personali o familiari, i permessi sindacali di cui al CCNQ 4 dicembre 2017 e s.m.i., i permessi per assemblea, i permessi di cui all'art. 33 della legge 104/1992.

9 - In caso di problematiche di natura tecnica e/o informatica, e comunque in ogni caso di cattivo funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito o sensibilmente rallentato, il dipendente è tenuto a darne tempestiva informazione al proprio dirigente/responsabile. Questi, qualora le suddette problematiche dovessero rendere temporaneamente impossibile o non sicura la prestazione lavorativa, può richiamare il dipendente a lavorare in presenza. In caso
di ripresa del lavoro in presenza, il lavoratore è tenuto a completare la propria prestazione lavorativa fino al termine del proprio orario ordinario di lavoro.

10 - Per sopravvenute esigenze di servizio il dipendente in lavoro agile può essere richiamato in sede, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio e, comunque, almeno il giorno prima. Il rientro in servizio non comporta il diritto al recupero delle giornate di lavoro agile non fruite.

11 – Come previsto dall'art. 19 della L. n. 81/2017, il lavoratore può recedere dal presente accordo di lavoro agile presentando apposita nota al proprio

dirigente/responsabile, indicando le motivazioni, con un preavviso di almeno 30 giorni. Con le medesime modalità, il dirigente/responsabile può recedere dall'accordo, sempre con un preavviso di almeno 30 giorni. Tale termine è elevato a 90 giorni nel caso di lavoratori disabili. Il lavoratore e il Dirigente possono recedere dall'accordo senza preavviso in presenza di un giustificato motivo,
quale ad esempio:
a. gravi e reiterati inadempimenti del lavoratore rispetto alla disciplina fissata nel progetto e nell'accordo di
lavoro agile;
b. oggettive e motivate esigenze organizzative sopravvenute e non prevedibili;
c. sopravvenute e gravi esigenze personali del lavoratore;
12 - Al presente accordo viene allegata l'informativa sulla salute e sicurezza nel lavoro agile, nonché le disposizioni per il trattamento dei dati, alle quali il dipendente è tenuto ad attenersi durante lo svolgimento della propria attività lavorativa in modalità agile.

Data _____

Firma del Dirigente/Responsabile

Firma del dipendente

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 o 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 autorità 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.
E' 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. E' 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
• E' 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 _____ _____che Lei potrà contattare ai seguenti riferimenti: Telefono: _____ – E-mail: _____ - Indirizzo PEC: _____

li _____

Firma per esteso e leggibile per presa visione_____