

# COMUNE DI VICENZA

## **ISTRUZIONI DI LAVORO DA OSSERVARE DURANTE LE SESSIONI DI SMART WORKING (“LAVORO AGILE”) nell'ambito delle misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID -19**

Visto quanto disposto dall'art. 3 del DPCM 23/2/2020 “Disposizioni attuative del DL 23/2/2020 n. 6 recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19” e dell'art. 1 comma 6 del DPCM 11 marzo 2020 in tema di “lavoro agile”;

Si autorizza il personale assegnato al “lavoro agile” nell'ambito delle misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID -19 al trattamento dei dati personali secondo le modalità specificate nello specifico accordo individuale, prescrivendo le specifiche istruzioni a seguire, volte a garantire che il trattamento dei dati effettuato durante le sessioni di lavoro venga effettuato in sicurezza.

### **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**

### **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'Ente, 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
- I dispositivi personali messi a disposizione dall'utente devono essere equipaggiati almeno con sistemi antivirus e provvisti di tutti i più recenti aggiornamenti sicurezza del sistema operativo del dispositivo utilizzato
- 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 la 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

- verificare l'identità dell'operatore remoto (tramite conoscenza diretta o comunicazione preventiva)
- controllare se è autorizzato allo svolgimento dell'intervento (tramite preventiva apertura di ticket, autorizzazione, ...)
- presidiare la postazione durante l'intervento, a meno che non sia stato concordato diversamente.

#### **Credenziali di accesso:**

- Non utilizzare password riconducibili alla propria realtà personale (data di nascita, nomi di parenti ecc).
- Le credenziali personali di accesso ai sistemi non possono essere condivise e 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.

#### **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.

## **Informativa ai sensi Regolamento UE 2016/679 per il trattamento dei dati effettuato nell'ambito dell'iniziativa "Lavoro Agile" (legge 22 maggio 2017, n. 81)**

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) 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 dell'accordo individuale per la prestazione di "lavoro agile".

Il trattamento viene effettuato con finalità correlate alle gestione dei dati nel contesto dell'iniziativa "lavoro agile", come previsto dalla legge 81/2017 in combinato con il DPCM 4 marzo 2020, 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'ente 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.

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 impegni previsti nei suoi confronti dall'accordo.

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, nonché con riferimento al diritto di portabilità dei dati e 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.

## **CONTATTI**

Titolare del trattamento dei dati personali è il Comune di Vicenza, nella persona del Sindaco pro tempore, con sede in Corso A. Palladio, 98 – 36100 Vicenza che Lei potrà contattare ai seguenti riferimenti:– Tel. 0444/221111 – pec: [vicenza@cert.comune.vicenza.it](mailto:vicenza@cert.comune.vicenza.it)

Potrà altresì contattare il Responsabile della protezione dei dati al seguente indirizzo di posta elettronica: [dpo@comune.vicenza.it](mailto:dpo@comune.vicenza.it).