ISTRUZIONI PRIVACY AGLI INCARICATI DI LAVORO AGILE (LA)

Lo svolgimento del lavoro agile da parte dei dipendenti del Comune di Campolongo Tapogliano deve avvenire in conformità alla normativa vigente in materia di privacy - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e decreto legislativo n. 196/2003 come modificato dal decreto legislativo n. 101/2018.

Per la tutela della riservatezza con riferimento al LA il personale dovrà osservare le misure di sicurezza generali quali l'identificazione e l'utilizzo delle password di sistema per accedere, anche da remoto, alle risorse informatiche e ai programmi e quelle già previste nel registro della Struttura di appartenenza in relazione alle categorie di trattamento pertinenti alle mansioni rivestite, in quanto applicabili, cui si fa rinvio.

Vanno sempre osservate, altresì, le misure recate nell'autorizzazione al trattamento dei dati in qualità di incaricato, anch'esse già impartite dal responsabile della Struttura all'atto dell'autorizzazione, che si riportano di seguito, in quanto da tener sempre in considerazione poiché costituiscono il bagaglio essenziale di nozioni relative alla tutela della riservatezza da applicare in tutte le situazioni:

- effettuare sui dati solo le operazioni inerenti il proprio segmento di attività
- trattare i dati, attenendosi ai principi di liceità, correttezza, minimizzazione dei dati in relazione alle finalità specifiche del trattamento connesse allo svolgimento delle attività di ufficio (p.es. che tipo di minimizzazione effettuare, indicare se vi siano attività che necessitino del consenso per la loro liceità, etc.)
- conservare i dati per un periodo non superiore a quello strettamente necessario per gli scopi del trattamento
- impegnarsi alla riservatezza
- segnalare al responsabile o altro soggetto designato le eventuali anomalie riscontrate o violazioni dei dati
- non cedere, salvo che ai destinatari individuati nel registro, ad alcun soggetto, compresi gli interessati per i dati eccedenti i loro diritti, nemmeno in consultazione né in comunicazione né in diffusione, i dati conferiti o gestiti per l'effettuazione del servizio, salvo il rispetto dei diritti previsti dalla norma a favore dell'interessato.
- essere consapevole delle sanzioni penali, amministrative pecuniarie e dei profili di responsabilità civile in caso di mancato rispetto delle norme sulla protezione
- partecipare alla formazione obbligatoria che sarà erogata in materia
- rispondere tempestivamente per ogni informativa necessaria richiesta dal RIT, dal Titolare o dal RPD.
- evitare la perdita o la distruzione anche solo accidentale dei dati o della documentazione cartacea e proteggere i dati tramite le operazioni di back up secondo le indicazioni fornite dai sistemi informativi
- mantenere riservato e custodito il cartaceo contenente dati personali

Con riferimento all'ultimo punto che presenta maggiori rischi in modalità di LA è necessario prestare la massima attenzione durante il trasporto del materiale cartaceo nei locali dove si svolge il LA, curando:
di utilizzare materiale consono come ad esempio valigette chiuse con il lucchetto o quantomeno

- borse chiuse con la cerniera;
- impedire l'accesso o l'intrusione da parte di terze persone: familiari, amici, astanti (se in luogo pubblico);
- disporre di un armadio chiuso a chiave.

Particolare attenzione deve essere posta, inoltre, ai seguenti rischi che possono ricorrere nella modalità di LA, per i quali si forniscono le misure necessarie per contrastarli cui attenersi:

Rischio di violazione privacy in modalità di LA	Misura prescritta
L'accesso o l'acquisizione dei dati da parte di terzi non autorizzati	Utilizzo di password sicure da inserire ad ogni interruzione della sessione di lavoro in presenza di altre persone o comunque quando ci si trovi in luogo pubblico

Furto o perdita di dispositivi informatici	I dispositivi devono essere custoditi con attenzione e diligenza; In caso di furto o perdita immediata denuncia all'Autorità di PS e comunicazione al proprio responsabile e ai sistemi informativi anche per eventuale blocco delle credenziali; Protezione con password curando di non essere visto all'atto dell'inserimento e crittografia dei dati, ove possibile.
Deliberata o inconsapevole alterazione di dati personali da terze persone	Protezione accurata delle banche dati e dei supporti informatici da bambini, animali domestici e terze persone in generale
Impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.	Installazione di programmi antimalware predisposti dai sistemi informativi; Condivisione con i sistemi informativi nel caso tali programmi fossero installati autonomamente
Perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità	Ove possibile software di backup che crea copie incrementali dei file aperti e/o eventuale creazione di un “mirror” alla fine della giornata lavorativa. Nel caso tali programmi fossero autonomamente installati occorre la condivisione e/o approvazione dei Sistemi informativi
Divulgazione non autorizzata dei dati personali	Prestare attenzione alla fuga di notizie ed in ogni caso avvertire il Titolare e il DPO per le notifiche necessarie