Linee Guida
Sul trattamento di dati personali
nel contesto del lavoro a distanza – Smart Working

ART. 1 - OGGETTO E PRINCIPI GENERALI

Le presenti linee guida forniscono a dipendenti e collaboratori (di seguito anche per brevità **"dipendenti"**) indicazioni operative per una corretta gestione di dati personali, documenti ed in genere informazioni d'ufficio e istituzionali, nel contesto delle attività lavorative svolte al di fuori dei locali dell'ente (di seguito per brevità **"tele lavoro")**
Il presente documento integra le disposizioni del "regolamento sull'uso degli strumenti informatici" e delle procedure analoghe, che si intendono operanti, in quanto compatibili, anche nelle attività di tele lavoro.

ART. 2 - REGOLE PER I TRATTAMENTI INFORMATICI

Il Dipendente che svolge attività di tele lavoro e accede da remoto alle risorse informatiche dell'ente, quali ad esempio software gestionali, Posta Elettronica, cartelle e database, Desktop remoto, software dedicati di Smart Working ecc. (di seguito per brevità **"risorse remote"**) deve rispettare le seguenti istruzioni:

1) Le risorse remote devono essere utilizzate esclusivamente per rendere la prestazione lavorativa a distanza.

2) Le credenziali di accesso alle risorse remote (user name e password) sono personali e riservate e dovranno essere conservate e custodite dal Dipendente con la massima diligenza. L'utilizzo delle risorse remote spetta esclusivamente al Dipendente. Per nessun motivo si possono delegare attività di tele lavoro a colleghi, familiari, amici o altre persone. Si informa che le credenziali assegnate costituiscono strumento tecnico e giuridico di riferibilità al Dipendente dell'attività svolta al di fuori dei locali dell'ente, tramite le risorse remote. Il sistema informatico di gestione delle risorse remote conservano i *log* di utilizzo riferiti ad un account del Dipendente, come specificato nel regolamento sull'uso degli strumenti informatici, che sono utilizzabili per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente e per ogni altra finalità prevista dall'art. 3 comma 4 della L. 300/70.

3) L'accesso alle risorse remote può avvenire tramite propri PC, notebook, tablet, smartphone (di seguito per brevità **"Strumenti"**) che dovranno essere utilizzati in via prioritaria dal medesimo Dipendente. Se possibile, si consiglia di creare un profilo utente specifico. Nella gestione delle password di accesso agli Strumenti si invita a seguire le regole di sicurezza previste nel presente documento e nel regolamento sull'uso degli strumenti informatici. Si consiglia l'uso di reti wi-fi e collegamenti ad Internet direttamente riferibili al Dipendente.

4) Gli Strumenti utilizzati e i relativi sistemi operativi devono essere aggiornati all'ultima versione disponibile rilasciata. E' vietato l'uso di sistemi operativi per i quali è stato interrotto il rilascio degli aggiornamenti di sicurezza.

5) Gli Strumenti devono essere dotati di un programma antivirus aggiornato.

6) Le credenziali di accesso alle Risorse remote non devono essere memorizzate nello strumento, tramite funzionalità che permettono di "salvare" la password di accesso per non doverla digitare nuovamente al successivo accesso (divieto di funzioni di log-in automatico).

7) Non lasciare incustoditi appunti scritti con le credenziali di accesso alle risorse remote (fogli nei pressi dello strumento, post-it affissi allo schermo ecc.) e non inviare la password per e-mail. Se si dovesse essere costretti a scrivere una password, si invita a conservarla in luogo sicuro o di

sostituirne alcune parti con descrizioni personali, codici ecc. E' necessario prestare attenzione a non essere visti mentre si digita la password di accesso Al termine delle necessarie operazioni o in caso di allontanamento anche temporaneo dallo Strumento utilizzato per il tele lavoro, il Dipendente è tenuto obbligatoriamente a chiudere il proprio account effettuando il log-out (Disconnetti).

8) E' vietato salvare documenti e atti di lavoro sui propri Strumenti Personali o su memorie rimuovibili personali (Chiavette USB, Memory Card ecc.).

9) Il dipendente che smarrisce le credenziali di accesso o rileva incidenti informatici o comportamenti anomali delle Risorse remote o degli Strumenti è tenuto a comunicare tempestivamente l'accaduto all'amministratore di sistema o al proprio responsabile.

ART. 3 REGOLE PER I TRATTAMENTI NON INFORMATICI

Il Dipendente anche nel contesto di tele lavoro è tenuto alla massima riservatezza, evitando di comunicare, diffondere, divulgare o riferire a soggetti non autorizzati informazioni e documenti lavorativi, seguendo le seguenti regole:

1) Non comunicare a nessun soggetto non specificatamente autorizzato documenti, dati e informazioni dei quali venite a conoscenza nell'esercizio dell'attività di telelavoro.

2) In caso di telefonate o videoconferenze su tematiche sensibili (che coinvolgano persone fisiche e relativi dati personali anche sanitari o particolari), si invita a ritirarsi in un luogo non accessibile a familiari o soggetti terzi.

3) Si invita a tenere in ordine la postazione di tele lavoro senza lasciare incustoditi appunti, fascicoli, documenti sensibili. Custodire con cura le stampe di materiale riservato. Non lasciate accedere alle stampe persone non autorizzate e, qualora risulti necessario eliminare documenti contenenti dati personali, si invita a sminuzzarli diligentemente.

ART. 4 - RINVIO AD ALTRE REGOLAMENTAZIONI

Per quanto non previsto nelle presenti linee guida, si rimanda al Regolamento sull'uso degli strumenti informatici e alla normativa vigente, in particolare al Reg. 679/16 - GDPR in materia di protezione dei dati personali.