DISCIPILNARE UTILIZZO STRUMENTI INFORMATICI E RISERVATEZZA DOCUMENTI CARTACEI PER SMART WORKING E DIDATTICA A DISTANZA (LE SEGUENTI REGOLE SONO STABILITE DA AGID)

Il dipendente in smart working o didattica a distanza è tenuto innanzitutto a:
- custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;
- al rispetto delle previsioni del Regolamento UE 679/2016 e del D.lgs. 196/2003 come modificato dal d.lgs. n. 101/2018 in materia di privacy e protezione dei dati personali.

In ottemperanza alle disposizioni comunitarie e nazionali nonché di contratto, il dipendente è tenuto alla più assoluta riservatezza sui dati e sulle informazioni in suo possesso e/o disponibili sul sistema informativo e conseguentemente dovrà adottare, in relazione alla particolare modalità della sua prestazione, ogni provvedimento idoneo a garantire tale riservatezza.

Inoltre, nella qualità di "autorizzato" del trattamento dei dati personali, anche presso il proprio luogo di prestazione fuori sede, dovrà osservare tutte le istruzioni e misure tecniche ed organizzative previste dall'azienda e di cui è già a conoscenza, avendo sottoscritto il disciplinare tecnico.

In particolare, con riferimento alle modalità smart work o didattica a distanza, dovrà:
- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione fuori sede;
- procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- qualora non si utilizzino dispositivi forniti dal titolare del trattamento si proceda ad installare almeno un buon sistema antivirus ed effettuare un'accurata scansione preventiva;
- evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili;
- adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come paraschermi (privacy-screen) che impediscano la visuale laterale del vicino, non tanto e solo per motivi di riservatezza, ma anche per la circolazione dei dati;
- evitare di rivelare al telefono informazioni di carattere personale;
- evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie;
- alla conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso la Sua abituale sede di lavoro;
- qualora, invece, al termine del lavoro risulti necessario trattenere presso il proprio domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

Nello specifico, quindi, il dipendente, dal punto di vista gestionale, in regime di smart working o didattica a distanza dovrà:
- Organizzare all'interno della propria abitazione una postazione di lavoro dedicata. Tale postazione dovrà disporre di appositi device, analogamente a quella lavorativa.
- Ridurre al minimo le interferenze di altri soggetti, eventualmente presenti nell'abitazione, in termini di rumore ed ingerenze/distrazioni.
- Rendere conto e ragione del proprio lavoro per dare e ricevere feedback; rendendosi presente ed efficiente, anche da remoto.

Per quanto concerne la sicurezza informatica, il dipendente dovrà attenersi alle seguenti procedure:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dall' Amministrazione/azienda.
   2. Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto.
   3. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo.
   4. Assicurasi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati.
   5. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dall' Amministrazione/azienda.
   6. Non installare software proveniente da fonti/repository non ufficiali.
   7. Bloccare l'accesso al sistema e/o configura la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro.
   8. Non cliccare su link o allegati contenuti in email sospette.
   9. Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette.
   10. Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dall' Amministrazione/azienda).
   11. Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si conclude la sessione lavorativa.

Sanzioni disciplinari:
La violazione, anche di una delle disposizioni precedenti, comporta un grave inadempimento disciplinare che prevede l'applicazione di sanzioni.
È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari, espulsivi e risarcitori previsti dal Contratto di lavoro sottoscritto ovvero dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

Luogo e data
Firma del dipendente per presa visione e accettazione

_____

Firma datore di lavoro o Legale rappresentante Ente

_____