REGIONE CALABRIA
Dipartimento Organizzazione e Risorse Umane
"Datore di Lavoro, Sicurezza Luoghi di Lavoro, Privacy – Rapporti con gli Enti locali e Polizia locale",

Catanzaro lì 16 marzo 2020
Prot. n. 110523 /SIAR

Trasmissione tramite PEC

A tutti i dipendenti

OGGETTO: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio ("GDPR") D.lgs. n.196/2003 e ss.mm.ii. – Principi comportamentali dipendenti in smart working.

Ad integrazione delle norme comportamentali richieste per tutti gli incaricati al trattamento in materia di protezione dei dati personali si forniscono le seguenti informazioni finalizzate ad assicurare che la prestazione lavorativa da svolgere in forma agile venga espletata nel rispetto dei principi di liceità, correttezza, riservatezza, dignità e moralità.

L'attività svolta in modalità smart working deve rispettare le medesime disposizioni e normative in materia di protezione dei dati personali già previste nell'ambito dell'attività svolta presso la sede di lavoro.

Il dipendente che accede al lavoro in modalità smart working deve essere consapevole che lo svolgimento di un'attività al di fuori della sede preposta comporta una maggiore attenzione nel preservare la confidenzialità e la riservatezza delle informazioni in suo possesso a cui potenzialmente possono avere accesso terzi non autorizzati.

Si ribadisce che, a norma di legge e di contratto, i dipendenti sono tenuti alla più assoluta riservatezza dei dati e delle informazioni in loro possesso e/o disponibili sui sistemi informativi regionali, e che, conseguentemente, gli stessi dovranno adottare, in relazione alla particolare modalità della loro prestazione, ogni provvedimento e misura idonei a garantire tale riservatezza.

Inoltre, nella qualità di "Incaricati del trattamento dei dati personali", anche presso il loro luogo di svolgimento della prestazione lavorativa fuori dalla sede ordinaria di lavoro, dovranno osservare tutte le misure di sicurezza previste nella relativa lettera di nomina di cui è già stata presa visione.

In considerazione della autorizzazione VPN con riferimento alla modalità smart working, il dipendente ha accesso fuori dall' usuale ambiente di lavoro a molteplici dati di proprietà regionale e, pertanto, si richiama ancor più l'attenzione sui seguenti punti:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di svolgimento della prestazione lavorativa fuori dalla sede ordinaria di lavoro proteggendo il dispositivo attraverso password da non trasferire a terzi;
- procedere a bloccare il dispositivo informatico/personal computer utilizzato in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- al termine della prestazione lavorativa giornaliera ed in ogni pausa di lavoro, è necessario conservare e custodire i documenti eventualmente stampati e tutta la documentazione relativa all'attività di lavoro;
- qualora occorra trattenere presso il luogo di svolgimento della prestazione in smart working documentazione cartacea contenente dati personali, quest'ultima al termine del lavoro, dovrà essere conservata in armadi, cassetti o altri contenitori muniti di serratura;
- utilizzare i sistemi ed i programmi informatici messi a disposizione dall'Amministrazione regionale nell'esclusivo interesse d'ufficio, non consentendo assolutamente ad altri l'utilizzo degli stessi. I sistemi devono essere protetti attraverso password di sistema da non trasferire a terzi. Si consiglia un rinnovo della password con cadenza settimanale.

Cordialmente

Il Dirigente di Settore
Dr. Salvatore Lopresti