OMAR
istituto tecnico industriale
Sede: 28100 Novara – B.do Lamarmora, 12

SMART WORKING E PROTEZIONE DEI DATI PERSONALI

Indicazioni operative per un corretto trattamento di dati personali nel contesto dello "smart working"

Con riferimento alla Circolare n. 1/2020 del 04/03/2020 ("Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa") emanata dal Ministro per la Pubblica Amministrazione, nella quale si dispone il ricorso in via prioritaria alle modalità di "lavoro agile" o "smart working" nel contesto delle misure di contenimento dell'emergenza epidemiologica da Covid-19, si fornisce una serie di indicazioni operative per il trattamento di dati personali effettuato con queste modalità di svolgimento della prestazione lavorativa.

Innanzitutto Lei dovrà svolgere i trattamenti previsti dalle sue mansioni nel rispetto delle prescrizioni e indicazioni operative contenute negli atti di individuazione quali **persona autorizzata al trattamento**, **ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati").**

Tali prescrizioni, aventi carattere "generico" anche allo scopo di adattarsi a situazioni emergenziali come quella in cui ci troviamo, sono perfettamente valide anche in un contesto di "smart working".

Nel rispetto della sopracitata circolare ministeriale e la conseguente esigenza di regolamentare modalità lavorative che, di fatto, costituiscono una novità per la pubblica amministrazione, comprese le istituzioni scolastiche, ribadiamo in questa sede alcuni concetti fondamentali e necessari al fine di effettuare un trattamento di dati personali conforme alla vigente normativa in un contesto di "smart working".

Indipendentemente dalle diverse concrete vie di implementazione dello "smart working", avendo necessariamente a che fare con dispositivi informatici, è necessario che Lei garantisca un adeguato livello di protezione di tali dispositivi, attenzionando in particolare il rispetto dei principi di **integrità**, **riservatezza** e **disponibilità** dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi.

A tale scopo occorre:

1. usare un pc/tablet in modo esclusivo o che abbia almeno un account dedicato e protetto da password;

2. proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e delle connessioni (cablate o Wi-Fi) attraverso l'uso di password sufficientemente robuste e sicure: a tal proposito si consiglia di utilizzare password lunghe in quanto più difficili da scoprire e prive di riferimenti ai dati anagrafici propri e dei familiari; ciò vale tanto per l'accesso ai propri dispositivi quanto per l'accesso a Internet, in quanto la diffusa prassi di non cambiare la password di default per l'accesso alla rete Wi-Fi è una delle principali cause di accessi non autorizzati alla rete locale e, di conseguenza, a dati e informazioni potenzialmente sensibili;

3. prediligere, ove possibile, l'utilizzo di sistemi di autenticazione a due fattori: Google permette di utilizzare l'autenticazione a due fattori per tutti i propri account, i quali sono la chiave di accesso, oltre agli account Android, anche agli strumenti di G Suite;

4. mantenere aggiornati sistemi operativi e software, sia desktop che mobile, utilizzati per svolgere la prestazione lavorativa: gli aggiornamenti sono importanti in quanto spesso risolvono falle di sicurezza sfruttabili per accedere ai dispositivi e ai dati in essi contenuti;

5. utilizzare e mantenere aggiornati specifici software antivirus e firewall, che offrono una tutela nei confronti dei rischi normalmente connessi alla navigazione in rete: i sistemi operativi Windows hanno integrati sia un software antivirus (Defender) sia un firewall;

6. implementare sistemi di backup per assicurare la disponibilità di dati e informazioni in ogni momento, sia tramite sistemi cloud che tramite dispositivi di archiviazione di massa come hard disk portatili e chiavette USB: in entrambi i casi l'accesso ai dati va protetto adeguatamente, magari servendosi di soluzioni crittografiche;

7. nel lavorare da casa è altresì importante attuare una serie di misure organizzative per svolgere le proprie mansioni in un ambiente lavorativo idoneo, come avere cura nell'impostare la propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari.

8. quando si accede ai programmi della Scuola le password non devono mai essere salvate sul pc e devono essere immesse ad ogni accesso;

9. non salvare alcun documento sul pc;

10. se si usano elenchi e tabelle contenti dati personali non devono essere mai salvati sul pc;

11. non possono essere portati a casa documenti in formato cartaceo originale.

12. In caso di lavoro da remoto e di accesso alla cartella di rete della scuola, è necessario che Lei dipendente acceda esclusivamente alle cartelle e ad i documenti che avrebbe potuto consultare stando in sede, e ciò in linea con quanto previsto nei documenti di autorizzazione al trattamento dati predisposti ad inizio anno.

Le indicazioni sopra esposte valgono per qualsiasi tipo di concreta applicazione dello "smart working".

Novara ……..

Il Dirigente Scolastico
Ing. Francesco Ticozzi

Il Dipendente

……