# 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 derivante dalla diffusione del coronavirus Covid-19, si forniscono una serie di indicazioni operative per il trattamento di dati personali effettuato con queste modalità di svolgimento della prestazione lavorativa.

Innanzitutto, i dipendenti devono svolgere i trattamenti previsti dalle rispettive mansioni nel rispetto delle prescrizioni e indicazioni operative contenute negli atti di individuazione quali persone autorizzate 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, è opportuno rammentare 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", impiegando necessariamente dispositivi informatici, è necessario che il lavoratore 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. **proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e alle connessioni (cablate o Wi-Fi) attraverso l'uso di password sufficientemente robuste e sicure. In tal senso è opportuno rammentare che:**

- Le password dovrebbero essere almeno di 8 caratteri, composte sia da caratteri alfanumerici (A-Z, 0-9) che da simboli o caratteri speciali (!, ?, @, ecc.), in quanto più difficili da decriptare. Il suggerimento basilare per la creazione di una password ottimale prevede che la stessa presenti almeno un carattere maiuscolo, un carattere minuscolo, un numero e un simbolo.
- Le password devono essere prive di riferimenti ai dati anagrafici propri e dei familiari, come anche dati di facile acquisizione quali numero di patente, carta d'identità o codice fiscale.
- È possibile creare ed usare password che richiamino proprie passioni o personaggi di fantasia in modo da ricordarle facilmente senza tuttavia essere insicure (es. Ferrari@F1).
- Si suggerisce di cambiare le password almeno ogni 6 mesi.
- Si suggerisce di utilizzare una password diversa per ogni dispositivo e\o account (es. Smartphone, tablet, piattaforme online, social network, account bancari, etc.)
- Si suggerisce di non trascrivere le password su supporti cartacei posti in evidenza (ad es. post-it collocato sulla scrivania, sul monitor, trascritta su un calendario).

**Dove possibile, la password può essere sostituita dall'uso dell'impronta digitale, se il dispositivo in dotazione lo consente (es. Smartphone). Ciò, in quanto tale sistema di accesso presenta maggior margine di sicurezza rispetto alle password.**

Quanto sopra esposto vale sia per l'accesso ai propri dispositivi che per l'accesso a Internet, in quanto la diffusa prassi di non cambiare la password di default per l'accesso alla rete, oppure l'abitudine ad impiegare la stessa password per più account o dispositivi, è frequente causa di violazione dei sistemi o della rete;

2. **Prediligere, ove possibile, l'utilizzo di sistemi di autenticazione a due fattori che, come lascia intuire il termine, sono sistemi composti da due elementi: credenziali dell'account quali nome utente e password e verifica ulteriore dell'identità, generalmente ottenuta mediante un dispositivo personale associato come lo Smartphone.**

**Una modalità di questo tipo viene impiegata da Google, che 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.**

3. **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; Nei sistemi di tipo Windows di recente rilascio (7, 8, 10) è presente l'aggiornamento automatico, se attivato. In via alternativa, è possibile procedere manualmente al download degli aggiornamenti.**

4. **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; È ovviamente possibile implementare antivirus e firewall di altri produttori quali, a titolo d'esempio: Avast, Kaspersky, Norton.**

5. **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, quando possibile, o limitando l'accesso a tali dispositivi solo al personale autorizzato. Una semplice misura di sicurezza consiste nell'impiegare l'hard disk esterno o la chiavetta USB solo quando necessario, evitando di lasciare il dispositivo collegato dopo l'uso. Altresì, chiudere in cassetti\armadi tali dispositivi quando non usati.**

6. **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.**

Le indicazioni sopra esposte valgono per qualsiasi tipo di concreta applicazione dello "smart working" ma, si precisa, sono valevoli anche in ambito di lavoro svolto con modalità tradizionale.

**Nel caso in cui la modalità di svolgimento della prestazione lavorativa "in smart working" è messa in atto tramite l'utilizzo dei propri dispositivi personali, così come riconosciuto nella circolare ministeriale citata, vista la cronica insufficienza disponibilità di risorse e strumenti informatici, tali indicazioni devono essere seguite con particolare rigore. Vanno altresì seguite nel caso in cui l'istituzione scolastica sia in grado di**

**fornire ai propri dipendenti dei dispositivi scolastici opportunamente configurati secondo le misure minime di sicurezza ICT per la PA.**

Passando a modalità di "smart working" più avanzate, si rammenta che nel caso in cui sia possibile per i lavoratori effettuare l'accesso alla rete interna della scuola dall'esterno, ciò va fatto necessariamente tramite una VPN, vale a dire un collegamento privato crittografato e, quindi, sicuro. Vanno evitate modalità che garantiscono standard di sicurezza molto inferiori come l'apertura di porte. Il vantaggio di accedere alla rete interna dell'Istituto è facilmente comprensibile, ma deve essere fatto in assoluta sicurezza.

Una soluzione che unisce le potenzialità di condivisione di dati e informazioni in tempo reale (così come avviene in un sistema server-client come quelli che caratterizzano le reti interne degli Istituti) e le possibilità di coordinamento, gestione e rendicontazione del lavoro svolto da remoto è quella di servirsi di servizi cloud, così come suggerito nella stessa circolare del Ministero. Servizi cloud come quelli messi a disposizione a titolo gratuito per le istituzioni scolastiche da Google e Microsoft – ma anche la suite Argo Software e le varie piattaforme di e-learning accessibili via web sono servizi cloud – sono potenti strumenti che permettono la gestione digitale dell'attività amministrativa e didattica delle istituzioni scolastiche. Anche in questo caso valgono le indicazioni di cui sopra, specialmente quelle riguardanti la robustezza delle credenziali per accedere a tali servizi.

Inoltre, quando ci si rivolge a servizi esterni, bisogna sempre ricordare che questi agiscono quali responsabili esterni del trattamento, ai sensi dell'art. 28 del RGPD: è ormai prassi consolidata che siano direttamente le grandi aziende a formalizzare questo tipo di rapporto nei contratti di servizio che si sottoscrivono alla registrazione, ma è sempre meglio verificare, leggendo attentamente la documentazione fornita.

**Napoli, 17/03/2020**

**Il Responsabile della Protezione dei Dati**

**Avv. Giuseppe Napolitano**