VOSTRO DPO:

info@formatori.eu <info@formatori.eu>
Lun 15/03/2021 23:02
A: CSIC80900L - IC ROSE L. DOCIMO <csic80900l@istruzione.it>

Regolamento UE 679/2016

SMART WORKING E PROTEZIONE DEI DATI PERSONALI

Oggetto: Indicazioni del Titolare dei Trattamenti e del Responsabile protezione dati

per un corretto trattamento di dati personali nel contesto dello "smart working" da recapitare ai dipendenti in attività lavorativa remota, ai sensi del Reg. UE 679/16 "GDPR in materia di Protezione dei Dati Personali" e della direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica a seguito dei DPCM 1 aprile 2020 in richiamo dei precedenti DCPM restrittivi anti-contagio "ulteriori misure di contenimento del Coronavirus Covid-19 e sospensione attività didattiche" nonché il Decreto 19 ottobre 2020 del Ministro per la pubblica amministrazione concernente la disciplina sul lavoro agile nell'emergenza e successivi (nota M.I. n. 1934 del 26.10.2020) relativi protocolli che hanno modificato ed integrato le misure anti-contagio Covid 19

In applicazione di quanto previsto dal D.P.C.M. del 1 aprile 2020 e della direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica, in seguito all'allarme Coronavirus e alle misure di prevenzione e controllo decise dal Governo per contenere e limitare il diffondersi del virus COVID-19, nonché il Decreto 19 ottobre 2020 del Ministro per la pubblica amministrazione concernente la disciplina sul lavoro agile nell'emergenza e successivi (nota M.I. n. 1934 del 26.10.2020) che si richiamano e intesi per trascritti e ripetuti emanati ad integrazione delle misure anti-contagio. Il decreto, all'articolo 4, comma 2, stabilisce infatti che "nei casi di quarantena con sorveglianza attiva o di isolamento domiciliare fiduciario, ivi compresi quelli di cui all'articolo 21-bis, commi 1 e 2, del decreto-legge 14 agosto 2020, n. 104, convertito con modificazioni, dalla legge 13 ottobre 2020, n. 126, il lavoratore, che non si trovi comunque nella condizione di malattia certificata, svolge la propria attività in modalità agile". Si comunica che i Dirigenti scolastici organizzano le attività necessarie concernenti l'amministrazione, la contabilità, i servizi tecnici e la didattica, avvalendosi prevalentemente (per quanto possibile) della modalità a distanza, secondo le modalità semplificate previste dalla Nota 6 marzo 2020, n. 278.

Si fornisce una serie di **indicazioni operative per il trattamento di dati personali** effettuato con queste modalità di svolgimento della prestazione lavorativa.

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, ribadiamo in questa sede alcuni concetti fondamentali e necessari al fine di effettuare un trattamento di dati personali conforme alla vigente normativa in un contsto di "smart working".

Indipendentemente dalle modalità di "smart working", avendo necessariamente a che fare con 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 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;

2. 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;

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;

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 sofware antivirus (Defender) sia un firewall;

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;

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". Nel caso in cui tale modalità di svolgimento della prestazione lavorativa è messa in atto tramite l'**utilizzo dei propri dispositivi personali**, così come riconosciuto nella circolare ministeriale alla quale facciamo riferimento vista la cronica non sufficiente 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.

Per 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 diffusa per la gestione e rendicontazione del lavoro svolto da remoto è quella di servirsi di **servizi cloud (software gestionali della scuola)**, così come suggerito nella stessa circolare del Ministero. 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 andare a verificare leggendo attentamente la documentazione fornita.

Si ricorda che Garante per la protezione dei dati personali ha indicato ai titolari del trattamento, quali le istituzioni scolastiche, di astenersi dall'effettuare **iniziative autonome di raccolta sistematica e generalizzata di dati riguardanti lo stato di salute dei lavoratori** che non siano normativamente previste o disposte dagli organi competenti. A riguardo, il Ministro per la Pubblica Amministrazione ha fornito indicazioni operative sull'obbligo per il dipendente pubblico di segnalare all'amministrazione la provenienza da un'area a rischio.

Ulteriori raccomandazioni:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dalla Amministrazione di appartenenza;
2. Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
3. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;
4. Assicurarsi 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 dalla Amministrazione di appartenenza;
6. Non installare software proveniente da fonti/repository non ufficiali;
7. Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando vi si allontana 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 dalla propria Amministrazione);
11. Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la propria sessione lavorativa.

In effetti il dipendente (assistenti amministrativi e/o lavoratore/trice in telelavoro) in smart working è tenuto innanzitutto a:

- custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;
- si chiede agli assistenti amministrativi e/o lavoratore/trice in telelavoro o smart working di mantenere tutti gli obblighi di riservatezza quale incaricato/referenti al trattamento dei dati dell'Ente Scuola in conformità al Regolamento UE 679/16, conservazione in sicurezza e mantenimento in segretezza delle password personali di accesso alla piattaforma, custodire in modo protetto e non accessibile a tutti i terminali utilizzati per espletare il telelavoro e che i dati non siano accessibili a persone non autorizzate e non divulgarli, se non per quelle esclusive finalità istituzionale legale all'Ente Scuola che rimane titolare del Trattamento.

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.

In particolare, con riferimento alle modalità smart - work, dovrà:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo diprestazione fuori sede;
- procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, ancheper un intervallo molto limitato di tempo;
- qualora non si utilizzino dispositivi forniti dal titolare del trattamento si proceda ad installare almeno unbuon sistema antivirus ed effettuare un'accurata scansione preventiva;
- evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili;
- 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 dilavoro;

- qualora, invece, al termine del lavoro risulti necessario trattenere presso il proprio domicilio materialecartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

Dati di contatto del **DPO**: Altomari Carmine – altomaricarmine@gmail.com

Titolare Trattamento Dati: I.C. DOCIMO ROSE, Dirigente Scolastico CONCETTA SMERIGLIO

email: csic80900l@istruzione.it

Si ricorda che tutte le informative sui trattamenti sono consultabili sul sito web della scuola, le nomine a incaricato sottoscritte in fase contrattuale sono comprensive di autorizzazione al trattamento dei dati di segreteria, certo nel rispetto di tutto quanto detto sopra.

Il Dirigente Scolastico

CONCETTA SMERIGLIO

Firma autografa sostituita a mezzo stampa

ai sensi dell'art. 3 comma 2 del D.L. 39/93