UNIVERSITÀ DEGLI STUDI FIRENZE

ISTRUZIONI PER LA PROTEZIONE DEI DATI PER IL PERSONALE IN SMART WORKING A CAUSA DELL'EMERGENAZA CORONA VIRUS

A seguito dell'emanazione del DL 17 marzo 2020 n. 18 il lavoro agile è da considerarsi la modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni fino alla cessazione dello stato di emergenza epidemiologica da COVID-2019, per questo si ritiene utile fornire 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 generali e indicazioni operative pubblicate nell'Intranet di Ateneo nella sezione "Protezione Dati – Privacy", in quanto Incaricati del Trattamento e autorizzati a compiere operazioni di trattamento dei dati detenuti dalle strutture di afferenza.

Tali prescrizioni, aventi carattere "generico" sono perfettamente valide anche in un contesto di smart working, tuttavia data la natura emergenziale ed improvvisa degli ultimi provvedimenti normativi che hanno reso il lavoro agile la modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni fino alla cessazione dello stato di emergenza epidemiologica da COVID-2019, è opportuno rammentare alcuni concetti fondamentali e necessari al fine di effettuare un trattamento di dati personali conforme alla vigente normativa in un contesto di smart working.

Nell'eseguire la prestazione lavorativa in smart working, essendo impiegati necessariamente dispositivi informatici, è necessario che il dipendente garantisca un adeguato livello di protezione di tali dispositivi, prestando particolare attenzione al rispetto dei principi di integrità, riservatezza e disponibilità dei dati e delle informazioni, per minimizzare 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 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.
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- 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);
- le password vanno cambiate almeno ogni 6 mesi;

- è consigliato utilizzare una password diversa per ogni dispositivo e\o account (es. Smartphone, tablet, piattaforme online, social network, account bancari, etc.);
- le password non vanno annotate su supporti cartacei posti in evidenza (ad es. post-it collocato sulla scrivania, sul monitor, trascritta su un calendario);
- La password non va **mai** divulgata a nessuno, nemmeno agli amministratori dei sistemi.

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

La diffusa prassi di non cambiare la password per l'accesso alla rete, oppure l'abitudine ad impiegare la stessa password per più account o dispositivi, sono cause frequenti causa di violazione dei sistemi o della rete.

Si ricorda che l'accesso ai sistemi e servizi on line dell'Università sono accessibili con le credenziali uniche di Ateneo che non vanno comunicate a nessuno. La posta elettronica e l'accesso alla G Suite di Ateneo richiedono un'autenticazione specifica. Il login si effettua con USERNAME e PASSWORD.

2. 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. Per garantire l'accesso agli ultimi aggiornamenti di sicurezza, è necessario utilizzare sistemi operativi per i quali è attualmente garantito il supporto dal produttore.

3. Utilizzare e mantenere aggiornati software antivirus e firewall, che offrono una tutela nei confronti dei rischi normalmente connessi alla navigazione in rete: i sistemi operativi Windows 8, 8.1, 10 hanno integrati sia un software antivirus (Defender) sia un firewall. È ovviamente possibile implementare antivirus e firewall di altri produttori (vedi SMART WORKING KIT servizi, strumenti e software per il personale UniFI pubblicate all'indirizzo https://www.unifi.it/upload/sub/comunicazione/smart_working_kit_personale.pdf).

4. Salvare i dati i per assicurare la disponibilità di dati e informazioni in ogni momento utilizzando i sistemi cloud messi a disposizione dell'Ateneo (G drive, file service OLMO e TIGLIO).

Qualora fosse necessario utilizzare dispositivi di archiviazione di massa come hard disk portatili e chiavette USB prediligere modelli che utilizzano sistemi di crittografia dei dati. In ogni caso si raccomanda di, evitare di lasciare i dispositivi collegato dopo l'uso e chiuderli in cassetti\armadi quando non usati.

5. Nel lavorare da casa è importante mettere in atto misure organizzative per svolgere le proprie mansioni in un ambiente lavorativo idoneo, per cui bisogna prestare particolare attenzione nell'impostare la propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari.

Se lo smart working è effettuato con dei dispositivi personali dei dipendenti, tali indicazioni devono essere seguite con particolare rigore.

Per accedere in modo sicuro ad internet attraverso la rete di Ateneo i dipendenti possono attivare la VPN (Virtual Private Network, una rete privata virtuale che garantisce privacy, anonimato e sicurezza attraverso un canale di comunicazione riservato) messa a disposizione da Siaf (vedi SMART WORKING KIT servizi, strumenti e software per il personale UniFI pubblicate all'indirizzo https://www.unifi.it/upload/sub/comunicazione/smart_working_kit_personale.pdf).

Altri accorgimenti per assicurare la protezione dei dati lavorando in smart working :

- Distruggere qualsiasi documento lavorativo venga stampato a casa;
- Non salvare documenti di ufficio sul pc personale, se non temporaneamente e poi cancellarli immediatamente (specie se contengono informazioni personali);
- Porre attenzione nell'inviare foto o schermate del PC;
- L'accesso a dati aziendali non è più pericoloso in smart working, la pericolosità dipende da come lo strumento e l'operatore gestiscono il dato, non dalla locazione della persona.

Altri suggerimenti utili:

a) http://www.funzionepubblica.gov.it/lavoro-agile-e-covid-19/linee-guida;

b) https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza.

Il Responsabile per la Protezione Dati

(Dott. Massimo Benedetti)