SMART WORKING

ELEMENTI ESSENZIALI PER LA PIANIFICAZIONE DI SMART WORKING E TELELAVORO NEL RISPETTO DELLA NORMATIVA PRIVACY

M2 INFORMATICA

M2 INFORMATICA SRL

Il nostro team di consulenti IT e privacy si occupa di studiare ed implementare soluzioni tecnologiche innovative, offrendo servizi in ambito **ICT Governance**, **ICT Security** & **GDPR Compliance.**

Il nostro **obiettivo** è fornire alle aziende un interlocutore capace di collaborare con il management attraverso la consulenza di specialisti di cyber security, esperti di GDPR compliance e sviluppatori software, per assicurare la conformità alla normativa e un adeguato livello di sicurezza.

Il know how acquisito in anni di esperienza ci consente di offrire una gamma completa di **servizi e prodotti** per la protezione dei dati personali e aziendali.

INTRODUZIONE

Cosa devo fare se voglio attivare lo smart working?

Lo smart working è uno strumento che negli ultimi anni è diventato molto semplice da gestire, ma occorre **pianificare** le modalità di lavoro da remoto e **individuare** le aree chiave su cui è necessario focalizzare l'attenzione.

Bisogna ricordare, inoltre, che il GDPR ricomprende un ambito molto più ampio rispetto ai temi di seguito affrontati.

Esistono dei rischi connessi al lavoro da remoto?

Le soluzioni che permettono di impostare il lavoro da remoto comportano molteplici rischi per l'azienda e per i diritti dei dipendenti: se non opportunatamente valutato in ottica di gestione del rischio, lo smart working potrebbe provocare un aumento degli errori umani, con **rischio di perdita** o **modifica non autorizzata** di dati.

Cosa c'entra il lavoro da remoto con il GDPR?

Il GDPR impone **specifici obblighi** per la sicurezza dei dati trattati dall'azienda.

Le soluzioni tecnologiche adottabili per consentire il lavoro da remoto comportano **il trattamento di dati personali** (compresi anche quelli dei dipendenti), che deve essere realizzato nel rispetto del GDPR.

Il lavoro da remoto, quindi, è un'attività che necessita di un'attenta pianificazione per ridurre i rischi sia sotto **il profilo cybersecurity** che sotto quello **privacy.**

Per una **corretta pianificazione** dell'attività di smart working bisogna prestare attenzione alle seguenti aree chiave:

- Gestione delle misure organizzative
- Gestione delle misure tecniche
- Rispetto dei principi di liceità, correttezza e trasparenza

LE PRINCIPALI MISURE ORGANIZZATIVE

Definizione di una politica interna

Lavorare da remoto non significa semplicemente dotare di un pc portatile i dipendenti, ma definire una **politica interna** che tenga conto di 3 punti essenziali:

- Condizioni per l'accesso alle risorse aziendali
- Modalità di collegamento alle risorse aziendali
- Limiti di utilizzo degli strumenti di lavoro

Oltre a stabilire delle regole specifiche, è necessario anche **formare le persone** in merito ai rischi connessi allo smart working.

Tra **i rischi più comuni** quando si lavora da remoto:

- Furto o abuso delle credenziali di accesso ai sistemi informativi e servizi informatici aziendali
- Maggiore esposizione a virus e malware e tentative di phishing
- Maggiore esposizione a vulnerabilità software
- Maggiore tendenza a commettere errori, in assenza di confronto diretto con i colleghi

Non sottovalutare i rischi

Molto spesso per lavorare da remoto viene consentito l'accesso alle risorse aziendali attraverso **connessioni poco sicure** (come wi-fi pubblici o non protetti), che potrebbero essere sfruttate per permettere intrusioni ai sistemi informativi aziendali.

Oltre formare tutte le persone che lavorano da remoto per renderle consapevoli di tali rischi, sarebbe opportuno fornire loro un **hotspot wi-fi mobile** configurato in modo sicuro, sulla base delle policy interne all'azienda.

Allo stesso modo, è auspicabile informare i dipendenti di **evitare di lavorare in luoghi pubblici**, dove il monitor del pc su cui si sta lavorando è maggiormente esposto a sguardi di malintenzionati che potrebbe fraudolentemente acquisire informazioni riservate.

Fornitori di servizi e Data Processing Agreement

Le soluzioni tecniche utilizzate per agevolare il lavoro da remoto spesso sono di tipo software as a service: coloro che forniscono tali soluzioni sono dei **Responsabili del trattamento** (in base all'art. 28 del GDPR) e ciò comporta una serie di conseguenze giuridiche e informatiche.

Il Titolare del trattamento deve rivolgersi soltanto a Responsabili che presentino **garanzie** sufficienti per dimostare l'adeguatezza delle proprie **misure di sicurezza**. In mancanza di tali garanzie il Titolare potrebbe essere chiamato a rispondere in solido anche in caso di violazioni di legge commesse dal fornitore.

Occorre, poi, verificare l'adeguatezza delle clausole contrattuali previste nel contratto di fornitura del servizio, affinché contengano tutte le disposizioni previste dall'art. 28 del GDPR. In assenza, sarà necessario un contratto integrativo, ossia un **Data Processing Agreement.**

LE PRINCIPALI MISURE TECNICHE

La flessibilità e l'autonomia che il lavoro da remoto offre comportano anche dei rischi, che sono tuttavia gestibili se vengono preventivamente analizzati durante la fase di pianificazione.

Come accedere alle risorse aziendali

Se le risorse aziendali non sono in Cloud, per accedervi da remoto ci sono due alternative possibili: utilizzare una **connessione VPN** o installare un **software per il controllo remoto.**

La VPN (Virtual Private Network) **è una connessione privata** con cui il dipendente può collegarsi, da remoto, direttamente alle risorse aziendali e lavorare come se fosse alla sua scrivania. Le connessioni tramite VPN sono cifrate ed ogni utente deve essere autenticato.

Il software per il controllo remoto, invece, permette di connettersi e gestire il computer tramite un altro computer, collegato al primo grazie all'accesso remoto.

È necessario accertarsi che tali software forniscano un controllo centralizzato degli accessi per evitare rischi di accesso non autorizzato ai sistemi aziendali.

Dispositivi aziendali o personali?

Il **rischio è variabile** a seconda che si utilizzino dispositivi forniti direttamente dall'azienda o dispositivi personali.

La motivazione è semplice: i dispositivi personali si differenziano notevolmente tra loro, e la loro configurazione è al di fuori del controllo dell'azienda.

I dispositivi personali dei dipendenti potrebbero avere un sistema operativo non aggiornato (o addirittura obsoleto) o dei **software** installati **che comportano rischi** per la sicurezza informatica dell'azienda.

Sistema operativo e antivirus

Se l'utilizzo di dispositivi personali per il lavoro da remoto è stato autorizzato, è necessario accertarsi che questi soddisfino dei **requisiti minimi di sicurezza**.

Il pc deve avere un **sistema operativo aggiornato** con patch di sicurezza e **licenza antivirus**: in caso contrario potrebbe essere opportuno dotare il pc di licenza per l'installazione del software, o fornire al dipendente un pc aziendale configurato in modo sicuro.

Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al dispositivo rappresentano **una delle principali criticità**, specialmente se viene consentito l'utilizzo di un pc personale.
Tali credenziali devono essere gestite in maniera adeguata poiché, oltre i rischi segnalati precedentemente, c'è la possibilità che il **dispositivo personale** venga usato **in ambito familiare**, aumentando maggiormente i rischi di abuso delle credenziali di accesso.

Nel caso in cui i dipendenti abbiano necessità di accedere a risorse particolarmente importanti per l'azienda, sarebbe opportuno implementare tecniche di autenticazione multi- fattore, così da ridurre il rischio di abuso delle credenziali di autenticazione e accesso non autorizzato ai sistemi aziendali.

Gestisci le identità digitali

Verifica periodicamente **le credenziali d'accesso** dei dipendenti, registrandole in un apposito registro e revocandole quando necessario (ad esempio in caso di assenza prolungata dal lavoro).

Verifica periodicamente le **autorizzazioni di accesso ai sistemi aziendali** secondo il principio di minimizzazione del GDPR.

Accertati che i **privilegi d'accesso** degli amministratori di sistema siano monitorati.

Un'occasione per fare ordine

La pianificazione del lavoro da remoto può rappresentare un'occasione per **censire** e **pre-autorizzare** tutti i dispositivi che si connetteranno alla rete aziendale o ai servizi informatici necessari per il lavoro.

Tale gestione risulta essere particolarmente utile per **controllare** il perimetro aziendale che, in un frangente come il lavoro da remoto, è necessariamente distribuito e geograficamente esteso.

DIRITTO DEL LAVORO E PRIVACY

Il controllo a distanza dei dipendenti è un'attività regolata sia dalla normativa in materia di diritto del lavoro (art. 4 dello Statuto dei Lavoratori) sia dalla normativa privacy (GDPR).

Posso controllare i dipendenti che lavorano da remoto?

Solo rispettando alcune regole.

Per prima cosa occorre ricordare che, in linea di principio, **controllare l'attività dei dipendenti non è consentito** né dallo Statuto dei Lavoratori, né dal GDPR, né dal Garante della Privacy italiano.

Sono previste, tuttavia, **alcune eccezioni**: l'utilizzo di strumenti da cui deriva la possibilità di controllo a distanza dei lavoratori è possible solo **per esigenze organizzative, produttive, e di sicurezza,** previa autorizzazione dell'Ispettorato del Lavoro territorialmente competente o tramite accordo con le rappresentanze sindacali aziendali.

Ciò non vale per gli strumenti di lavoro, o la registrazione delle presenze: in tali casi I dipendenti potranno essere monitorati anche senza le due precedenti condizioni.

.

Quali sono gli strumenti di lavoro?

Tutti I dispositivi che costituiscono un mezzo indispensabile al lavoratore per eseguire la prestazione lavorativa, e che per tale finalità sono messi a sua disposizione. Alcuni esempi per chiarire il concetto:

Videosorveglianza: non è uno strumento necessario per eseguire la prestazione lavorativa .

GPS: a seconda del contesto può essere considerato o meno uno strumento indispensabile per l'esecuzione della prestazione lavorativa.

Email aziendale: la posta elettronica è considerata uno strumento di lavoro e, rispettando I principi di liceità, correttezza e trasparenza di cui sotto, può essere oggetto di controllo.

Non è sempre facile capire se si è in presenza di uno strumento di lavoro: deve essere considerato lo specifico contesto aziendale e gli specifici software utilizzati, che spesso sono delle vere e proprie soluzioni integrate che formano un sistema complesso e variegato.

Liceità correttezza e trasparenza

Il datore di lavoro non può utilizzare i software aziendali, le webcam e altre tecnologie per capire se lo smart worker è collegato al suo computer o se si trova in casa.

Il datore di lavoro può svolgere **controlli** mirati, anche a distanza, a patto che siano **proporzionati e non invasivi**, e che **riguardino beni aziendali** (il pc fornito dal datore, la casella di posta aziendale) rispetto ai quali il dipendente non ha alcuna aspettativa di segretezza.

Occorre però **informare** i dipendenti in anticipo del fatto che gli strumenti che l'azienda mette a disposizione per il lavoro da remoto non possono essere usati per motivi personali.