

LO SMART WORKING PREVENZIONE E PROTEZIONE



LO SMART WORKING...TUTELATO

In questo momento sociale, decisamente delicato, che ci troviamo, nostro malgrado, a dover vivere per fronteggiare la pandemia da Covid-19, siamo stati obbligati per il bene di tutta la comunità, a dover accettare ed affrontare cambiamenti alla nostra routine quotidiana in ambito privato ed in ambito lavorativo.

Restare tra le mura di casa, senza possibilità di svago all'aperto, o senza la possibilità di un aperitivo tra amici, o una pizza in famiglia, sono alcune delle restrizioni a cui abbiamo dovuto abituarci nella nostra sfera privata.

Cosa è cambiato in ambito lavorativo?

Le aziende hanno dovuto rivedere completamente il loro modello di business, mettendo in atto misure drastiche per poter rallentare e impedire l'espandersi del contagio (tra queste ricordiamo: la chiusura di attività non necessarie ai beni primari, la turnazione del personale impiegatio...ecc)

E cosa dire dello SMART WORKING?

Lo Smart Working, più precisamente, può essere definito come quell'"insieme di modelli organizzativi, moderni e non convenzionali, caratterizzato da un elevato livello di flessibilità nella scelta degli spazi, degli orari e degli strumenti di lavoro, e che fornisce a tutti i dipendenti di un'azienda le migliori condizioni di lavoro". Tale specifica modalità di svolgimento della prestazione lavorativa è stata inserita all'interno di un quadro normativo italiano per la prima volta con la **legge 81/2017**, il famoso "Job Act".

Ai lavoratori agili viene garantita la parità di trattamento - economico e normativo - rispetto ai loro colleghi che eseguono la prestazione con modalità ordinarie.



È, quindi, prevista la loro tutela in caso di infortuni e malattie professionali, secondo le modalità che sono illustrate dall'INAIL nella Circolare n. 48/2017.

A partire dal 15 novembre 2017 le aziende potranno sottoscrivere accordi individuali con i lavoratori che decidono di usufruire della modalità di lavoro agile e dovranno procedere all'invio di tali accordi attraverso l'apposita piattaforma informatica messa a disposizione sul portale dei servizi del Ministero del Lavoro e delle Politiche Sociali (l'obbligo di accordo scritto con il lavoratore è temporaneamente sospeso per il periodo emergenziale da Covid-19).

Nell'invio dell'accordo individuale dovranno essere indicati:

- i dati del datore di lavoro
- i dati del lavoratore
- la tipologia di lavoro agile (tempo determinato o indeterminato)
- la durata del lavoro agile.

Ma cosa serve ad un lavoratore per poter operare a distanza?

Semplice:

- strumenti tecnologici per poter effettuare l'attività lavorativa in modalità agile;
- una rete wi-fi;
- un collegamento costante con team e colleghi per poter avanzare nell'operatività del lavoro.

Quali sono le principali problematiche correlate al ricorso allo smart working?

Lo smart working richiede una riorganizzazione lavorativa, finalizzata a proseguire da casa le attività che prima venivano svolte in ufficio. Il lavoro agile risulta quindi una sfida sia per le aziende, che per i lavoratori stessi, poiché richiede di fronteggiare diverse novità da assorbire in pochissimo tempo. Sarà necessario in particolare prestare **sempre maggiore attenzione a tutto ciò che riguarda la Cyber Security e la protezione dei propri dati nonché gli aspetti relativi alla sicurezza sul lavoro.**

Cosa fare per proteggere i propri dati?

Le minacce informatiche a cui ci si espone lavorando da casa aumentano esponenzialmente, soprattutto a causa dei dispositivi personali non adeguatamente protetti (incluse connessioni di rete: ADSL, WiFi, ecc.), utilizzati per accedere ai sistemi aziendali. Spesso infatti, quando si utilizzano strumenti non forniti dall'azienda, le misure di sicurezza vengono trascurate e si sottovalutano i rischi connessi alla navigazione in rete.

In uno scenario come questo, la possibilità di utilizzare computer infetti da malware, di cadere vittima di intercettazioni di comunicazioni o di perdere i dati a causa di attacchi informatici, incrementa particolarmente.



Alcuni esempi di gestione che possono essere messi in atto dall'azienda e dall'utente in materia di protezione informatica sono:

- Aggiornamento dei sistemi informatici
- Cifratura dei sistemi elettronici usati per il lavoro
- Utilizzo di periferiche esterne
- Protezione delle videoconferenze e delle comunicazioni
- Scelta di password con alti livelli di protezione
- Adozione di sistemi anti-intrusione
- Rapida segnalazione dei problemi.

Per le aziende è essenziale inoltre implementare soluzioni di protezione complete ed integrate, verificando accuratamente e periodicamente lo status dei dispositivi e gli aggiornamenti di programmi e app.

Riveste un ruolo altresì importante la formazione dei dipendenti sugli aspetti fondamentali della Cybersecurity e sulla gestione efficiente delle situazioni di rischio informatico. **Non basta avere gli strumenti giusti, bisogna anche saperli utilizzare.**

Come deve essere gestito l'aspetto della sicurezza sul lavoro?

Nonostante le difficoltà oggettive del momento e del lavoro a distanza e da remoto, non dobbiamo dimenticarci della tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro, o in questo caso: **in Smart Working.**



È infatti, sempre, responsabilità del Datore di Lavoro, come prevede la legge 81/2017 con l'articolo 22, garantire la tutela della salute e della sicurezza dei propri dipendenti.

L'Art. 22 riporta quanto segue:

1. *"Il datore di lavoro garantisce la salute e la sicurezza del lavoratore che svolge la prestazione in modalità di lavoro agile e a tal fine consegna al lavoratore e al rappresentante dei lavoratori per la sicurezza, con cadenza almeno annuale, un'informativa scritta nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro."*;
2. *"Il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali"*.

Cosa deve effettivamente fare, in concreto, il datore di lavoro per adempiere a quanto sopraccitato?

Tra gli obblighi del datore di lavoro all'art. 18 comma 1 lett "l" del Dlgs 81/08 e s.m.i. troviamo: *"adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37"*; pertanto, il datore di lavoro dovrà redigere un'informativa contenente tutte le informazioni relativamente ai rischi connessi all'attività lavorativa svolta in un ambiente domestico.



Di seguito viene riportato un elenco esemplificativo e non esaustivo dei rischi e delle misure che devono essere necessariamente considerate:

- Rischio videoterminale legato ad una postazione di lavoro munita di schermo in riferimento alle caratteristiche del computer portatile, tablet o smartphone in dotazione;

- Rischio ergonomico in riferimento ad una postazione tipo, dotata di equipaggiamento quali: sedia a 5 razze girevole, poggiatesta ecc,



- utilizzo sicuro dei telefoni cellulari / smartphone / cordless e dei rischi legati agli eventuali campi elettromagnetici a cui il soggetto potrà essere esposto durante la normale attività lavorativa (o domestica);
- rischi elettrici in riferimento ai requisiti e corretto utilizzo di impianti di alimentazione elettrica;
- rischio microclimatico relativamente all'ambiente indoor in cui può essere svolto il lavoro in modalità Smart Working;
- Eventuali riferimenti ad utilizzo obbligatorio di cuffiette per dispositivi smartphone al fine di evitare esposizioni a radiazioni di apparati tecnologici;
- Eventuali riferimenti a pause obbligatorie per legge, ai fine di evitare sovraccarico visivo.

Esiste un problema sociale legato al ricorso allo smart working?

Datore di lavoro e lavoratore possono stabilire che la prestazione lavorativa – anche con forme di organizzazione per fasi, cicli e obiettivi nonché senza precisi vincoli di orario o di luogo di lavoro – venga eseguita “(...) in parte all’interno di locali aziendali e in parte all’esterno senza una postazione fissa”.

Il tutto, purché entro i limiti di durata massima dell’orario di lavoro giornaliero e settimanale derivanti dalla legge e dalla contrattazione collettiva.

Successivamente all’entrata in vigore della Legge 81/2017, infatti, all’interno di alcuni CCNL si è iniziato a disciplinare l’utilizzo degli strumenti di lavoro nel rispetto della prestazione lavorativa, garantendo il diritto del lavoratore ai tempi di riposo giornaliero e settimanale, ai periodi di ferie e agli altri legittimi casi di assenza.

Possiamo quindi dire che ciascun lavoratore che ricorra alla modalità di lavoro abbia diritto alla disconnessione.

Questo interessamento delle parti sociali e politiche per il diritto alla disconnessione è dovuto anche al fatto che il lavoratore a cui non sia consentito esercitarlo sarebbe esposto al rischio di tecnostress, ovvero la sindrome che colpisce l’individuo che deve gestire forme di conoscenze complesse e i flussi informativi offerti dalle nuove tecnologie. **Il tecnostress è stato riconosciuto nel 2007 come malattia professionale a seguito di una sentenza emessa dalla Procura del Tribunale del Torino.**

Sul tema, infine, si è espresso anche il Garante della Privacy Italiano in audizione al parlamento il 13 maggio 2020 affermando che “è necessario assicurare in modo più netto il diritto alla discussione per tutelare la distanza tra spazi di vita privata e attività lavorativa”.

“Non sarebbe legittimo - continua Soro - fornire per lo smart working un computer dotato di funzionalità che consentono al datore di lavoro di esercitare un monitoraggio sistematico e pervasivo dell’attività compiuta dal dipendente tramite questo dispositivo”.



NOVITÀ



Il Gruppo 2G ha voluto sviluppare una **nuova proposta** in grado di offrire alle Aziende/Clienti un insieme coordinato di strumenti che consentano **nuove modalità di info-formazione a distanza** sia per fronteggiare questa crisi globale che per allinearsi con l'evoluzione che il mondo sta affrontando.

I **WEBINAR** proposti dal Gruppo 2G hanno l'obiettivo di un confronto diretto tra i relatori e le Aziende iscritte.

Il webinar proposto dal Gruppo 2G è completamente **GRATUITO** e si terrà:

MARTEDÌ 06 ottobre 2020 dalle h 15.00 alle h 15.20

Titolo: "Lo Smart Working – Prevenzione e Sicurezza"

Per partecipare compilate la scheda adesione che trovate di seguito e inviatela via mail a:

c.gagliardo@gruppo2g.com

DATI AZIENDA	Ragione Sociale Azienda _____
	Partita IVA/Cod. Fiscale _____
	Attività azienda _____
	Indirizzo Azienda _____
	Telefono _____ Fax _____
	E-mail _____
DATI PARTECIPANTE	Cognome/Nome _____
	Ruolo _____

Alcune semplici indicazioni per partecipare ai ns. webinar:

WEBINAR ACCESSIBILI DA PC, MACINTOSH, TABLET E SMARTPHONE, con accesso a internet, che dispongano di microfono e altoparlanti. Browser consigliati: Google Chrome, Mozilla Firefox, ...

Nella speranza che la nostra proposta sia di Vostro interesse e che possa rappresentare un momento formativo/informativo importante, oltre ad essere un'occasione di incontro e condivisione anche se virtuale ...



Dott. Ing. MARCO BROVERO

- Responsabile Area Automotive & Privacy del Gruppo 2G S.p.A.
- Auditor di prima e seconda parte ai sensi della UNI EN ISO 19011:2018
- Esperto privacy (Privacy Manager)



Dott.ssa MARTINA MASTRANTUONO

- Responsabile Area Health & Safety del GRUPPO 2G S.p.A.
- Incarichi di "RSPP" esterno
- Esperta in redazione di sistemi UNI ISO 45001: 2018
- Esperta in materia ambientale e di Sicurezza secondo D.Lgs. 81/08 e smi



Per avere maggiori informazioni sui nostri servizi potete contattare il ns. Ufficio Marketing (Sig.ra Cristina Gagliardo) che fisserà un appuntamento con uno dei ns. responsabili.

Tel. 011.5620022 c.gagliardo@gruppo2g.com

