Euroconference
Editoria

LA CIRCOLARE TRIBUTARIA

Settimanale di aggiornamento e approfondimento professionale in area tributaria

Speciale

Smart working

Smart working & privacy

di Andrea Onori – dottore commercialista e revisore legale

Cos'è lo *smart working*?

Se mi avessero fatto questa domanda qualche mese fa probabilmente la risposta non sarebbe stata precisa e consapevole come ora.

Il Lavoro agile è disciplinato dalla L. 81/2017.

Entrata in vigore a metà giugno dello stesso anno, la legge introduce misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi di lavoro subordinato.

La definizione di lavoro agile (*smart working*) la si trova nel comma 1, articolo 18, L. 81/2017 che recita:

> *"Modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e* ***senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici*** *per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita,* ***in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa****, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva".*

Dalla lettura della stessa emergono chiari i tratti (evidenziati in grassetto e sottolineati) determinanti per inquadrare e delineare gli aspetti rilevanti ai fini *privacy* o meglio della tutela del trattamento dei dati.

Prima di procedere in tale direzione si ritiene doveroso fare una piccola premessa che serve per delineare il contesto socio economico in cui è esploso il "fenomeno" dello *smart working*.

Oggi è diventato praticamente la modalità di prestazione di lavoro "normale" o quanto meno sta assumendo tale caratteristica.

Questo perché, nell'ambito delle misure adottate dal Governo per il contenimento e la gestione dell'emergenza da contagio da coronavirus Covid-19, il necessario distanziamento sociale e l'imposta sospensione delle attività produttive lo ha reso praticamente l'unica modalità di prestazione di lavoro subordinato ammessa.

Siamo stati catapultati in questo nuovo modo di lavorare per effetto delle prescrizioni di cui agli allora D.P.C.M. dell'8 marzo 2020 (articolo 2, comma 1, lettera r)) e dell'11 marzo 2020 (articolo 1, comma 1,

n. da 6) a 10)), oggi entrambi abrogati per effetto del D.P.C.M. 10 aprile 2020 che ha "ripreso" tali indicazioni.

Veniva stabilito rispettivamente che:

1. la modalità di lavoro agile può essere applicata per la durata dello stato di emergenza dai datori di lavoro a ogni rapporto di lavoro subordinato nel rispetto dei principi dettati dalle disposizioni in materia, anche in assenza di accordi individuali previsti; gli obblighi informativi di cui all'articolo 22, L. 81/2017 sono assolti in via telematica anche ricorrendo alla documentazione resa disponibile dall'Inail (D.P.C.M. 8 marzo 2020);

2. le P.A. assicurano lo svolgimento in via ordinaria delle prestazioni lavorative in forma agile del proprio personale dipendente, anche in deroga agli accordi individuali e agli obblighi informativi ...;

In ordine alle attività produttive e alle attività professionali si raccomanda che sia attuato il massimo utilizzo da parte delle imprese di modalità di lavoro agile per le attività che possono essere svolte al proprio domicilio o in modalità a distanza ... (D.P.C.M. 11 marzo 2020)

La disciplina oggi in vigore per effetto del D.P.C.M. 10 aprile 2020, per contro, prevede che:

> *"gg) fermo restando quanto previsto dall'articolo 87, D.L. 18/2020, per i datori di lavoro pubblici, la modalità di lavoro agile disciplinata dagli articoli da 18 a 23, L. 81/2017, può essere applicata dai datori di lavoro privati a ogni rapporto di lavoro subordinato, nel rispetto dei principi dettati dalle menzionate disposizioni, anche in assenza di accordi individuali previsti; gli obblighi di informativa di cui all'articolo 22, L. 81/2017, sono assolti in via telematica anche ricorrendo alla documentazione resa disponibile sul sito dell'Inail.*
>
> ...
>
> *ii) in ordine alle attività professionali si raccomanda che:*
>
> *1. sia attuato il massimo utilizzo di modalità di lavoro agile per le attività che possono essere svolte al proprio domicilio o in modalità a distanza;*
>
> ..."

Pertanto, con l'emergenza per il contenimento del contagio da coronavirus Covid-19, il Governo ha incentivato questa forma di lavoro "agile" su tutto il territorio nazionale al fine di contenere, o meglio, evitare/limitare gli spostamenti per motivi di lavoro, che, ogni giorno, erano causa di aggregazione e sovraffollamento (nei treni e negli autobus), prevedendone la possibilità di applicazione da parte dei datori di lavoro, pubblici e privati, a ogni tipologia di rapporto di lavoro subordinato, per tutta la durata dello stato di emergenza, anche in carenza degli "*accordi individuali previsti*" e ricorrendo alla documentazione messa a disposizione dall'Inail per adempiere agli obblighi di informativa (di seguito

il *link* da cui è possibile scaricare l'informativa in parola:

https://www.inail.it/cs/internet/comunicazione/avvisi-e-scadenze/avviso-coronavirus-informativa.html)

Smart working: gli elementi caratterizzanti rilevanti per la *privacy*

Come abbiamo evidenziato in precedenza, il lavoro "agile" ovvero il lavoro "da remoto" è caratterizzato dai seguenti aspetti:

– che la "*modalità di esecuzione del rapporto di lavoro subordinato [avvenga] senza vincoli [...] di luogo di lavoro*";

– che sia previsto il "*possibile utilizzo di strumenti tecnologici*";

– dal fatto che "*la prestazione lavorativa viene eseguita [...] in parte all'esterno*" [dell'azienda];

– che il lavoratore svolga la sua attività "*senza una postazione fissa*".

Passiamo, ora, in rassegna le caratteristiche di ogni aspetto sopra elencato.

Modalità di esecuzione del rapporto di lavoro subordinato senza vincoli di luogo di lavoro

Tale fattore caratterizzante rileva in ambito di tutela del trattamento del dato con riferimento al fatto che, non essendoci un vincolo riferito a un luogo di lavoro preciso, i documenti, i dati e le informazioni, oggetto della prestazione lavorativa, non possono essere raccolte, registrate, organizzate, modificate, consultate, utilizzate e conservate in un unico posto di lavoro "fisico", delimitato nello spazio con certezza e pertanto dotato di quegli accorgimenti strutturali e tecnici di sicurezza che un datore di lavoro deve adottare in funzione delle occorrenti "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al [...] regolamento*" (articolo 24, GDPR 679/2016).

Si palesa, quindi, una prima problematica rispetto alla necessaria (seppur limitata e controllata) necessità di trasferimento della documentazione analogica e/o informatica in un luogo diverso dalla sede "fissa" di lavoro messa a disposizione dal Datore di lavoro, Titolare del trattamento dei dati.

Possibile utilizzo di strumenti tecnologici

Tale aspetto, a parere di chi scrive, è elemento essenziale e imprescindibile dell'esecuzione di tale modalità di prestazione di lavoro subordinato, al punto tale da ritenere "superflua" o addirittura "errata" l'indicazione del "*possibile utilizzo di strumenti tecnologici*".

Perché?

Premesso che chi scrive ritiene ridondante la spiegazione della motivazione, la stessa, oggettivamente, e senza tema di errore e/o contestazione, la si trova nell'essenza della modalità di svolgimento della prestazione ovvero nella necessaria presenza di una dotazione *hardware* e *software*, sia in capo al prestatore di lavoro subordinato "agile" (*smart-worker*) sia in capo all'azienda, oltre che di un opportuno collegamento/interconnessione *internet* tra la postazione extra-aziendale del lavoratore e la sede del *Server* dell'azienda per la trasmissione, l'elaborazione dei dati, oltre che l'invio e, se del caso, la diffusione degli stessi.

Si sta facendo riferimento ad aspetti che fino a un mese fa, magari, ne avevamo solo sentito parlare e non li concepivamo come essenziali, se non addirittura, non li ritenevano efficaci per eseguire la nostra prestazione lavorativa.

Abbiamo dovuto familiarizzare con concetti quali VPN (*Virtual Private Network*), condivisione *in cloud*, linee guida sulla *Cyber Security*.

A molti di noi tutto ciò era oggettivamente ed effettivamente conosciuto nella teoria, ma sicuramente non adottato e utilizzato nella pratica, per contro altri, quelli più evoluti tecnologicamente, avevano già le dotazioni tecniche *hardware* e *software*, ma non erano utilizzate fattivamente.

Oggi tutto è cambiato, oggi tutto si è evoluto.

Il Covid-19 ci ha spinto verso una effettiva evoluzione tecnologica.

Anche nei momenti di maggiore difficoltà si possono cogliere gli aspetti positivi.

Abbiamo assistito a un salto tecnologico al quale non avremmo mai assistito in un arco temporale così breve.

Tutti, Pubblica Amministrazione e privati, hanno concretizzato una parte del progresso tecnologico che fino a qualche mese fa forse avevamo previsto e pianificato, ma mai avremmo pensato di attuarlo così rapidamente, anche a causa di una mancanza di progresso culturale nazionale.

Il CAD (Codice dell'Amministrazione Digitale) è una realtà da oltre 15 anni oramai, ma solo adesso, costretti, abbiamo realizzato la ineluttabilità di dover utilizzare le tecnologie per non fermarci.

Per continuare a lavorare e a produrre, abbiamo, come si dice, fatto il passo.

Siamo diventati tutti "*smart-worker*", anche i nostri ragazzi.

Con l'avvento della scuola digitale, oramai, anche loro, hanno familiarizzato con piattaforme digitali dove incontrarsi tra loro e con i professori assistendo alle video-lezioni, a familiarizzare con strumenti che permettono di effettuare video-chiamate per continuare a parlare e a relazionarsi con i propri compagni di classe, a inviare e ricevere *mail*, scaricare documenti e caricare informazioni e dati.

Lo *smart-worker* per lavorare da casa di cosa ha bisogno?

Di un *computer* e di un collegamento *internet*, come minimo.

Entrambe queste dotazioni, in tema di misure di sicurezza, hanno una indubbia rilevanza in materia di tutela del trattamento dei dati.

Il primo, il *computer*, assume rilevanza in quanto lo stesso può essere o una dotazione *hardware/software* di proprietà del datore di lavoro assegnata al dipendente o una dotazione "privata" del lavoratore.

In entrambi i casi cerchiamo di tracciare gli aspetti rilevanti ai fini *privacy*.

Computer di proprietà del datore di lavoro, dato in dotazione al dipendente

In questo caso l'*asset* rientra nella strumentazione di proprietà del datore di lavoro e sarà dotato di tutti quei componenti *hardware* e *software* quali unità esterne di *back-up*, *firewall* (fisici e virtuali), *antivirus*, gestionali aziendali, *software* di proprietà industriale, CMR oltre che *password* di accesso e *account* di posta elettronica secondo le politiche di sicurezza adottate dal Datore di Lavoro. Lo stesso sarà preimpostato per avere accesso tramite VPN alla rete aziendale come se fosse nella sua postazione di lavoro in azienda (Ipotesi sicura, in linea con le norme sulla *Cyber Security* e con le prescrizioni di cui al GDPR);

Computer di proprietà del dipendente

In questo caso l'*asset* non rientra tra la strumentazione del datore di lavoro e pertanto, ove presenti *policy* aziendali in tema di sicurezza, questo strumento non può essere ritenuto "sicuro" (mancanza di *white list* relative a *software* installati, presenza di *antivirus* non ritenuti adeguati, mancanza di limitazioni all'accesso a *internet*, presenza di *software/app* che inviano dati all'esterno, assenza di accesso esclusivo al *computer* (perché utilizzato da altri soggetti in famiglia), mancanza di un accesso sicuro alla casella di posta elettronica dell'ufficio, mancanza di un collegamento VPN *standard*), (Ipotesi non sicura e non in linea con le norme sulla *Cyber Security* e le prescrizioni del GDPR).

Il secondo, il collegamento a *internet*.

Tale aspetto tecnologico, nelle Attività professionali e aziendali di piccole dimensioni, può comportare il sostenimento di costi di sviluppo interni quali l'acquisto di un *server* idoneo a supportare un collegamento VPN, nonché la presenza di personale IT che sia in grado di gestire la rete con i relativi accessi, autorizzazioni e impostazioni di sicurezza nella consapevolezza che la delocalizzazione degli utenti della rete (*client*) e la moltiplicazione degli accessi virtuali comporta un incremento del rischio di violazione del sistema e pertanto della tutela dei dati aziendali.

Il collegamento *internet* serve per la comunicazione e la condivisione dei dati. Strada alternativa alla VPN per riuscire a condividere con i colleghi dati, informazioni e documenti è il "*Cloud*" ovvero la c.d. "*Nuvola*".

Dovendo interagire con il lavoro di altri abbiamo imparato a utilizzare spazi di archiviazione differenti dal *server* aziendale o di Studio, spazi di archiviazione virtuali, che possano essere raggiunti da più persone poste in luoghi diversi attraverso una connessione *internet*.

Tutti i documenti, la corrispondenza e i *software* sono condivisi, non archiviati e gestiti nei "nostri" *server*, ma in appositi "spazi virtuali" concessi dai *Provider* di servizi *cloud*. Società create e strutturate per gestire e conservare dati e informazioni di terzi (dotate, almeno si spera, di misure di sicurezza in merito alla prevenzione da perdita dei dati (previsione di *back-up* periodici e sistematici), nonché da accessi non autorizzati).

La prestazione lavorativa viene eseguita (...) in parte all'esterno (dell'azienda)

Questo terzo aspetto caratterizzante, pone dei problemi circa il necessario trasferimento della documentazione (tutta o in parte) oggetto dell'attività lavorativa, sia nel caso di documentazione analogica sia nel caso di documentazione digitale.

Nel primo caso (documentazione cartacea) mediante il trasporto fisico di tutto quanto il necessario dalla sede dello studio o dell'azienda per la prosecuzione delle pratiche in corso e per la prosecuzione di quelle successive ove non sia possibile procedere in altro modo.

Associato a tale fattispecie vi è un pericolo di perdita accidentale dei dati, di accesso non autorizzato e di diffusione non consentita.

Nel secondo caso (documentazione informatica), nel caso non vi sia un collegamento VPN, si deve fare attenzione ai salvataggi che vengono fatti nel corso della prestazione lavorativa e all'invio degli allegati, che necessariamente risiederanno nel *computer* utilizzato dallo *smart-worker* (lavoratore agile). Anche in tale seconda fattispecie risiede immanente il pericolo di perdita accidentale del dato o sottrazione del dato a causa anche dello smarrimento del computer o della memoria esterna.

(as)senza (di) una postazione fissa

Tale peculiarità porta alla luce il fatto che lo strumento tecnologico adottato sarà, nella stragrande maggioranza dei casi, un supporto *hardware* c.d. "portatile" che, per caratteristica intrinseca, è facile da spostare, perché la prestazione lavorativa deve essere svolta in luoghi diversi dalla sede/postazione "fissa" aziendale.

Smart working: accordo e controllo aziendale

La norma prevede che la prestazione lavorativa, effettuata mediante la modalità del lavoro agile, sia preceduta da un accordo in forma scritta che definisca:

1. le modalità di lavoro;
2. l'esecuzione della prestazione lavorativa svolta all'esterno dei locali aziendali, anche con riguardo alle forme di esercizio del potere direttivo del datore di lavoro e agli strumenti utilizzati dal lavoratore;
3. i tempi di riposo del lavoratore;
4. le misure tecniche e organizzative necessarie per assicurare la disconnessione dalle strumentazioni tecnologiche di lavoro.

Tali aspetti devono pertanto tradursi nella predisposizione di "Linee Guida" relative al comportamento che lo *smart-worker* deve adottare per esplicare la sua attività di lavoro subordinato al di fuori dell'azienda, all'esercizio del potere direttivo del datore di lavoro e indicazioni in merito agli strumenti da utilizzare, nonché le misure tecniche e organizzative necessarie (anche per assicurare la disconnessione dalle strumentazioni tecnologiche di lavoro in modo corretto e sicuro).

Devono pertanto essere indicate:

1. modalità e linee di condotta sull'utilizzo delle dotazioni aziendali (*computer/fax/* stampanti/*smartphone/laptop/tablet*);
2. gli accorgimenti e le precauzioni da adottare in merito alla protezione e custodia dei dispositivi mobili dati in dotazione;
3. la custodia e la gestione delle credenziali (ID e *password*) che consentono l'accesso tramite VPN al *server* aziendale e pertanto a dati riservati;
4. le modalità operative per un utilizzo corretto e sicuro dell'antivirus (preinstallato nel pc consegnato o da installare nel pc di proprietà del lavoratore);
5. le modalità da osservare per il salvataggio dei *files* e documenti;
6. da ultimo, ma non per questo meno importante, indicazioni relative all'utilizzo e alla gestione dell'*account* di posta elettronica aziendale e sull'utilizzo di *internet*;
7. le condotte, connesse all'esecuzione della prestazione lavorativa all'esterno dei locali aziendali, che danno luogo all'applicazione di sanzioni disciplinari;
8. l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore agile.

Si ritiene utile un approfondimento in merito a quanto indicato al:

– punto 2: occorre evidenziare che, ai fini di un corretto utilizzo delle applicazioni tramite l'uso di un *computer*, sarebbe opportuno rappresentare tale buon comportamento di utilizzo ai fini di una maggiore sicurezza inerente l'uso degli strumenti informatici "in dotazione" oppure "di proprietà" dello *smart worker*.

Ad esempio, l'utilizzo di un sistema di gestione dei dati e dei documenti in "*Cloud*" prevede per l'accesso allo spazio virtuale la fase di "*log-in*" con l'inserimento delle credenziali (*User* ID e *password*), ma occorre fare attenzione a un piccolo, ma importante passaggio tecnico.

Di solito il "*browser*" tende a memorizzare le credenziali (è presente una "finestra di dialogo" dove viene richiesto se memorizzarle o meno).

È buona norma rifiutare la memorizzazione delle stesse e ogni volta che si abbandona l'area della "*nuvola*" è opportuno farlo eseguendo la fase di "*log-out*" prima di chiudere il *browser*, perché, se questo passaggio non avviene, altri utenti che utilizzeranno il pc potranno accedere direttamente ai dati.

Rispettare le procedure informatiche di accesso e di uscita dalle varie applicazioni evita quello che, per la normativa in materia di tutela del trattamento del dato, viene definito "*Data Breach*" ovvero una violazione del trattamento dei dati per effetto di un accesso non autorizzato.

Tale ultima evenienza (*Data Breach*) deve essere prevista e disciplinata mediante la predisposizione di una apposita procedura, come previsto dal Regolamento Europeo in materia di *privacy*.

La procedura deve essere conosciuta dai lavoratori "agili" (*smart worker*), dovendo questi ultimi attuare e attivare la stessa nel caso in cui si verificasse una violazione.

– punto 8: la L. 81/2017 ha previsto all'articolo 21 che il potere di controllo all'esterno dei locali aziendali venga esercitato nel rispetto di quanto disposto dall'articolo 4, L. 300/1970 (Statuto dei lavoratori).

Inoltre, la stessa prevede che il datore di lavoro debba garantire la salute e la sicurezza del lavoratore consegnando al dipendente e al rappresentante dei lavoratori per la sicurezza un'informativa scritta (almeno una volta all'anno) nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro (articolo 22, L. 81/2017) e che il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

Il controllo dei lavoratori "agili". Come e quando?

Abbiamo, poco sopra, evidenziato che il controllo può essere effettuato, ma nel rispetto dell'articolo 4, Statuto dei lavoratori.

L'articolo in parola disciplina due diverse tipologie di "strumenti".

Al comma 1:

> *"Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per:*
>
> *- esigenze organizzative e produttive;*
>
> *- per la sicurezza del lavoro;*
>
> *- per la tutela del patrimonio aziendale.*
>
> *E possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. [...]. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato Nazionale del Lavoro [...]."*

Al comma 2:

> *"La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa [...]"*

Mentre al comma 3 viene previsto che:

> *"Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.Lgs. 196/2003",* e oggi anche del Regolamento Europeo 679/2016.

Si ritiene utile, per i fini del presente contributo, focalizzare l'attenzione sul comma 2, articolo 4, L. 300/1970 cercando di definire gli strumenti di lavoro, così da rientrare nel rispetto della previsione normativa che conduce a una sostanziale eliminazione delle restrizioni.

Oggi, gli "*strumenti di lavoro*" aziendali più diffusi sono telefoni, pc e *tablet.*

Questi tipi di "dotazioni", date in uso al personale dipendente, possono essere utilizzate senza l'accordo con le associazioni sindacali o l'autorizzazione della delegazione territoriale dell'INL (Ispettorato nazionale del lavoro).

Con riferimento al lavoratore "agile" (*smart worker*) i giustificati motivi che permettono i controlli sono le evidenti "*esigenze organizzative*" oltre alla "*tutela del patrimonio aziendale*", patrimonio che si può identificare nelle dotazioni aziendali fornite al lavoratore (*software*, CRM e/o Gestionali), presenti all'interno del pc, nonché tutti i dati "riservati" relativi al *marketing*, alla Ricerca & Sviluppo, ai dati personali dei dipendenti utilizzati per lo svolgimento della prestazione di lavoro "agile".

Pertanto, negli specifici contesti sopra indicati, il datore di lavoro può controllare il lavoratore a distanza per il tramite delle dotazioni tecniche e informatiche date in uso e utilizzare i dati e le informazioni acquisite per il tramite del controllo per "*tutti i fini connessi al rapporto di lavoro*" (scopi disciplinari, premiali, di produttività), fatto salvo il dovere di "*adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*".

Da quest'ultimo inciso discende la necessità (o meglio il dovere) di determinare e individuare, oltre che predisporre, una idonea e puntuale *policy* aziendale.

L'informativa:

1. definirà l'ambito e i confini in cui potranno essere utilizzate le informazioni dal datore di lavoro;
2. indicherà le modalità di utilizzo degli strumenti (con riguardo alle componenti *hardware*, *software*, nonché alle applicazioni) così da prevenire attivazioni fortuite, non volute, casuali, di funzioni da cui possa derivare un'attività di controllo nei confronti del lavoratore;
3. presenterà una "*white-list*" di programmi o applicazioni che sarà possibile installare e una "*black-list*" di programmi e applicazioni che non sarà possibile installare sugli strumenti aziendali;
4. indicherà le modalità di effettuazione dei controlli, elencando le applicazioni e i dati che saranno controllati, oltre che il possibile controllo da remoto dei dispositivi.

Riassumendo.

È possibile definire due categorie di strumenti:

1. di controllo;
2. di lavoro.

Con riferimento agli "strumenti di lavoro" il datore di lavoro può controllare e accertare inadempimenti contrattuali e illeciti disciplinari, ma non sempre è facile stabilire quando un dispositivo risponde a "*esigenze organizzative e produttive*" rispetto a quando lo stesso può essere utilizzato dal lavoratore per "*rendere la prestazione lavorativa*".

Nel primo caso vi è la necessità di una autorizzazione sindacale o amministrativa, nel secondo no.

Continuando il nostro approfondimento sul tema dello "*smart working*" il Garante è intervenuto, più volte nel tempo, perché spinto dall'evolversi del progresso tecnologico e soprattutto in considerazione dell'utilizzo sempre più massiccio, se non, oggi, esclusivo, degli strumenti informatici, oltre che di *internet*, nei processi di lavoro.

Si vuole richiamare, per la rilevanza delle indicazioni tecniche in esso contenute, il provvedimento n. 303/2016 in tema di utilizzo della posta elettronica e accesso a *internet* in considerazione della stretta attinenza della problematica con la concreta attuazione dello *smart-working*.

Oggi non è pensabile lavorare senza *mail* e senza connessione *internet*, nemmeno in azienda, figuriamoci da remoto.

Il Garante nel suo provvedimento ha evidenziato che:

> *"Quanto alle specifiche caratteristiche del trattamento dei dati derivante dalla configurazione del sistema, si ritiene che questo, articolandosi anche in operazioni di controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti internet esterni, peraltro registrati in modo sistematico e conservati per un ampio arco temporale, sia idoneo a consentire un controllo dell'attività e dell'utilizzo dei servizi della rete individualmente effettuato da soggetti identificabili".*

Oltre al fatto che:

> *"Il trattamento è effettuato, attualmente, per il tramite di apparati (differenti dalle ordinarie postazioni di lavoro) e di sistemi software che consentono, con modalità non percepibili dall'utente (c.d. in background) e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente), operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati degli accessi a internet o al servizio di posta elettronica".*
>
> *"Tali software non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell'articolo 4, comma 2, L. 300/1970, come modificato dall'articolo 23, D.Lgs. 151/2015; sul punto, cfr. nota del Ministero del lavoro e delle politiche sociali, del 18 giugno 2015; v. altresì la definizione di "attrezzatura" e "post[azione] di lavoro" di cui all'articolo 173 D.Lgs. 81/2008)".*
>
> *"In tale nozione, infatti - e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web - è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet".*
>
> *"Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore".*

Vengono di seguito indicati alcuni esempi, forniti dal Garante della *privacy*, di sistemi che costituiscono parte integrante degli strumenti indicati:

– sistemi di *logging* per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "*envelope*" del messaggio, per una breve durata non superiore comunque ai 7 giorni;

– sistemi di filtraggio antivirus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui *server* per l'erogazione dei servizi di rete;

– sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso.

> *"Altri strumenti pure utili al conseguimento di una elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controlli sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'articolo 4 Statuto dei lavoratori:*
>
> *- sistemi di protezione perimetrale – firewall – in funzione antintrusione*
>
> *- sistemi di prevenzione e rilevamento di intrusioni – IPS/IDS – agenti su base statistica o con il ricorso a sorgenti informative esterne".*

Oltre al Garante, anche il WP29 (Gruppo di Lavoro articolo 29 per la protezione dei dati) si è espresso sul tema del "trattamento dei dati nell'ambito del rapporto di lavoro" con il Parere 2/2017, adottato l'8 giugno 2017.

Il documento è stato rilasciato quando il GDPR 679/2016 era già entrato in vigore, ma non ancora applicabile (ricordiamo che ha iniziato ad avere effetti dal 25 maggio 2018) e comunque lo stesso è stato reso considerando le previsioni contenute nel Regolamento Europeo.

Il Parere vede la disamina di vari scenari di trattamento all'interno del rapporto di lavoro con il presupposto che lo stesso:

1. intende trattare tutte le situazioni di rapporto di lavoro, indipendentemente dal fatto che tale rapporto si basi su un contratto di lavoro;

oltre al fatto che:

2. la rapida adozione di nuove tecnologie dell'informazione sul posto di lavoro, in termini di infrastrutture, applicazioni e dispositivi intelligenti, consente nuovi tipi di trattamento sistematico dei dati sul posto di lavoro potenzialmente invasivi.

Tra le premesse viene evidenziato che il GDPR introduce, per i titolari del trattamento dei dati, 2 nuovi obblighi, previsti dall'articolo 25, ovvero quelli di "*attuare una protezione dei dati fin dalla progettazione* [*Privacy by Design*] e una *"protezione per impostazione definita"* [*Privacy by Default*]".

Lo stesso documento evidenzia, inoltre, come l'articolo 35 introduce l'obbligo, per il titolare del trattamento del dato, di:

> *"effettuare una valutazione di impatto sulla protezione dei dati quanto un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*

Nel Parere 2/2017 il Gruppo di Lavoro si è concentrato sull'inquadramento giuridico delle "*norme più specifiche per assicurare la protezione dei diritti e delle libertà, con riguardo al trattamento dei dati personali dei dipendenti, nell'ambito dei rapporti di lavoro*", evidenziando come l'articolo 88, GDPR presenti un elenco di finalità per cui tali norme specifiche possono essere emanate dai singoli Stati membri.

Si riporta per completezza l'elenco:

– assunzione;

– esecuzione del contratto di lavoro (compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi);

– gestione, pianificazione e organizzazione del lavoro;

– parità e diversità sul posto di lavoro;

– salute e sicurezza sul lavoro;

– protezione della proprietà del datore di lavoro o del cliente;

– esercizio e godimento (individuale) dei diritti e dei vantaggi connessi al lavoro;

– cessazione del rapporto di lavoro.

Viene successivamente fatto presente che tali norme devono includere:

> *"misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati".*

Con specifico riferimento:

– alla trasparenza del trattamento;

– al trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

– ai sistemi di monitoraggio sul posto di lavoro.

Con il documento in parola, il Gruppo di Lavoro fornisce le "Linee Guida" per l'uso legittimo di nuove tecnologie in una serie di situazioni specifiche, tra cui lo *smart working*, descrivendo nel dettaglio le misure appropriate e specifiche per la salvaguardia della dignità umana, il legittimo interesse e i diritti fondamentali dei dipendenti.

Molto interessante, poi, la profilazione dei rischi che evidenzia come le tecnologie moderne consentono di "tracciare" i dipendenti nel corso del tempo, nei luoghi di lavoro e nelle loro abitazioni, attraverso diversi dispositivi quali *smartphone*, *computer* da tavolo, *tablet*, veicoli e dispositivi indossabili.

Nel caso in cui il trattamento non sia soggetto a vincoli e non sia "trasparente" (palesato agli interessati) si configura un elevato rischio che il legittimo interesse del datore di lavoro al miglioramento dell'efficienza e alla protezione dei beni aziendali si trasformi in un monitoraggio ingiustificabile e intrusivo.

Le tecnologie che monitorano le comunicazioni e i comportamenti limitano i comportamenti naturali dei dipendenti, perché spinti a "conformarsi" per evitare possibili "ritorsioni", nonché gli stessi potrebbero essere inconsapevoli di quali dati vengono trattati, per quali finalità, ignorando, addirittura, l'esistenza della tecnologia di monitoraggio non potendo, quindi, esercitare i propri diritti.

Si riportano qui di seguito alcuni esempi di trattamento illegittimo effettuato mediante l'utilizzo di tecnologie:

– i sistemi che raccolgono dati relativi all'ubicazione tramite *wi-fi* con riferimento a una raccolta eccessiva dei dati;

– l'uso di sistemi legittimamente installati per proteggerei i beni aziendali per successive finalità di monitoraggio del rendimento dei dipendenti;

– Utilizzo di dati raccolti tramite un sistema di TVCC;

– Impiego dei dati di un sistema di geolocalizzazione per controllare costantemente i movimenti e il comportamento dei dipendenti (tracciamento wi-fi o *bluetooth*).

Da sempre, il monitoraggio delle comunicazioni elettroniche sul posto di lavoro (tramite telefono, navigazione *internet*, posta elettronica, messaggistica istantanea, VOIP) è stato considerato la minaccia principale.

Oggi, occorre tenere conto degli sviluppi tecnologici che hanno consentito nuove modalità di monitoraggio, potenzialmente più intrusive e pervasive, quali il monitoraggio di dispositivi personali che i dipendenti mettono a disposizione per lo svolgimento del loro lavoro in conformità con una specifica politica di utilizzo denominata *Bring-Yuor-Own-Device* (BYOD, ossia utilizza i tuoi dispositivi privati), nonché il ricorso alla tecnologia *Mobile Device Management* (gestione dei dispositivi mobili).

In tal caso, si evidenzia che l'azienda o l'organizzazione dovrà, alla luce dei principi contenuti nel Regolamento Europeo, essere in grado di dimostrare i propri concreti interessi legittimi all'utilizzo di strumenti informatici "invasivi" e potenzialmente lesivi dei diritti degli interessati.

Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione e della comunicazione al di fuori del posto di lavoro

Come indicato nel Parere 2/2017 mai come in questo ultimo periodo "*l'utilizzo delle tecnologie dell'informazione e della comunicazione, al di fuori del posto di lavoro, è diventato più comune*", ancora di più, oggi, per effetto delle indicate disposizioni di legge che prevedono la modalità di lavoro a distanza quale misura di contrasto alla diffusione del coronavirus Covid-19, anche mediante *"utilizzo dei propri dispositivi personali ("Bring Your Own Device")"*

Nel contempo, però, viene evidenziato che le:

> *"**funzionalità offerte da tali tecnologie possono rappresentare un rischio per la vita privata dei dipendenti**, in quanto spesso i sistemi di monitoraggio presenti sul posto di lavoro vengono estesi [...] alla sfera domestica dei dipendenti nel momento in cui questi utilizzano tali apparecchiature".*

Nel documento sono approfonditi importanti aspetti caratterizzanti la prestazione lavorativa in modalità "*smart working*", relativi a:

1. monitoraggio del lavoro a domicilio e del lavoro a distanza;
2. *bring your own device* (BYOD);
3. gestione dei dispositivi mobili (*mobile device management*).

Con riferimento all'analisi del primo punto.

1. Monitoraggio del lavoro a domicilio e del lavoro a distanza

La possibilità di lavorare da remoto implica che il datore di lavoro dia in dotazione ai propri dipendenti apparecchiature ICT o *software* che, una volta installati a casa o sui dispositivi personali, consentono ai dipendenti di avere lo stesso livello di accesso alla rete, ai sistemi e alle risorse del datore di lavoro di cui beneficerebbero se fossero sul posto di lavoro.

Sebbene possa essere uno sviluppo positivo, il lavoro a distanza presenta anche un rischio aggiuntivo per il datore di lavoro.

I dipendenti che hanno accesso da remoto all'infrastruttura aziendale non sono vincolati dalle misure fisiche di sicurezza che possono essere messe in atto presso i locali aziendali, pertanto, tutto ciò fa aumentare il rischio di accesso non autorizzato provocando la perdita o la distruzione di informazioni, ivi inclusi i dati personali dei dipendenti o dei clienti, che il datore di lavoro può conservare.

Al fine di attenuare tale rischio, i datori di lavoro potrebbero prevedere l'adozione di *software* in grado di registrare i tasti premuti e i movimenti compiuti dal *mouse*, di acquisire schermate visualizzate, di

registrare le applicazioni utilizzate (e la durata del loro impiego) nonché, su dispositivi compatibili, di attivare telecamere web e raccogliere così filmati registrati.

Ma tali tipi di scelte portano a un trattamento sproporzionato ed:

> *"è altamente improbabile che il datore di lavoro disponga di un fondamento giuridico e di un legittimo interesse per registrare i tasti premuti e i movimenti del mouse compiuti da un dipendente".*

Soluzioni?

> *"La chiave sta nell'affrontare il rischio posto dal lavoro a domicilio o a distanza in maniera proporzionata e non eccessiva".*

Con riferimento al secondo punto degli aspetti caratterizzanti lo *smart working*.

2. Bring your own device (byod)

I datori di lavoro possono trovarsi nella situazione di gestire le richieste di dipendenti che intendono utilizzare i loro dispositivi personali "sul posto di lavoro" per svolgere i propri compiti.

"*Bring Your Own Device*" (abbreviato in BYOD) indica appunto "*l'utilizzo di propri dispositivi personali*".

L'aspetto più problematico è, come facilmente intuibile, che il dispositivo del dipendente viene in parte usato per fini personali e in parte per la prestazione lavorativa.

Di conseguenza, esiste la possibilità concreta che l'uso di tali dispositivi comporti un trattamento, da parte dei datori di lavoro, di informazioni non aziendali relative a tali dipendenti ed eventualmente a qualsiasi loro familiare che utilizzi il dispositivo in questione.

Nei rapporti di lavoro, i rischi per la vita privata, derivanti dall'uso di dispositivi propri, sono comunemente associati a tecnologie di monitoraggio che raccolgono identificatori quali gli indirizzi MAC (*Media Access Control*), detti anche indirizzi fisici, indirizzi *ethernet* o indirizzi LAN, oppure ai casi in cui il datore di lavoro accede al dispositivo del dipendente con la giustificazione di effettuare una scansione per finalità di sicurezza, ad esempio, per rilevare la presenza di "*malware*"; in tali casi non si dovrebbe accedere alle sezioni del dispositivo che si presume vengano utilizzate esclusivamente per scopi privati (come la cartella dedicata alla conservazione di immagini scattate tramite il dispositivo).

Per contro, il monitoraggio dell'ubicazione e del traffico dati di tali dispositivi potrebbe rientrare nel legittimo interesse, del datore di lavoro, di proteggere i dati personali per i quali è responsabile.

Tuttavia, ciò diventerebbe illecito quando il trattamento (monitoraggio) riguarda un dispositivo personale di un dipendente e lo stesso permette di acquisire anche dati relativi alla vita privata e familiare.

I datori di lavoro dovrebbero attuare sistemi che consentano il trasferimento sicuro, tra il dispositivo del dipendente e la propria rete, dei propri dati presenti sul dispositivo. Il dispositivo dovrebbe, quindi, essere configurato in modo tale da indirizzare tutto il traffico attraverso una VPN in modo da offrire un certo livello di sicurezza; tuttavia, laddove utilizzi una simile misura, il datore di lavoro dovrebbe tenere conto del fatto che il software installato per finalità di monitoraggio costituisce un rischio per la vita privata del dipendente quando questi usa il dispositivo per fini personali.

Ultimo aspetto caratterizzante la modalità di prestazione lavorativa "agile/*smart*" è la

3. Gestione dei dispositivi mobili (mobile device management)

Consente ai datori di lavoro di localizzare i dispositivi, di installare configurazioni e/o applicazioni specifiche e di eliminare dati su richiesta.

I servizi di gestione dei dispositivi mobili consentono, inoltre, ai datori di lavoro di registrare o tracciare il dispositivo in tempo reale.

Prima di impiegare una simile tecnologia è necessario effettuare una valutazione d'impatto sulla protezione dei dati.

Se dalla valutazione emerge che la tecnologia di gestione dei dispositivi mobili è necessaria in specifiche circostanze, si dovrebbe in ogni caso effettuare una valutazione della conformità ai principi di proporzionalità e sussidiarietà del trattamento dei dati risultante.

È indubbio che sono sempre più diffuse tecniche e strumenti di monitoraggio del sistema informativo aziendale e sebbene le stesse possano garantire diversi livelli di sicurezza, non vi è dubbio alcuno che comportino, per contro, un abbassamento della tutela della *privacy* dei dipendenti che deve trovare il giusto bilanciamento.

Tecnologie quali "*Data Loss Prevention*", "*Next-Generation Firewalls*", "*Unified Threat Managment*", "*eDiscovery technologies*", "BYOD", possono essere sicuramente adottate e implementate, ma i dipendenti devono essere adeguatamente informati sul tipo di tracciamento attuato e sulle sue conseguenze nei loro confronti, nonché vi deve essere la previsione di diversi gradi di monitoraggio e ingerenza nella vita privata del lavoratore.

Conclusione

Per concludere il nostro approfondimento sugli aspetti *privacy* rilevanti per lo *smart working* si ritiene utile procedere con un elenco di sintesi degli adempimenti che il datore di lavoro dovrà porre in essere:

1. dare corpo ai principi di *privacy by design* e *privacy by default* nell'adozione della modalità di lavoro agile;

2. prevedere la minimizzazione dei dati (utilizzo solo di quelli necessari) nel rispetto dei principi di necessità, proporzionalità e pertinenza;
3. predisporre una apposita valutazione di impatto;
4. verificare, prima di consegnare le dotazioni al proprio personale, se nei dispositivi dati in uso al dipendente siano installati *software* che hanno finalità lecite, ma che permettono comunque un controllo a distanza del lavoratore e, nel caso, fare un accordo sindacale o richiedere l'autorizzazione all'INL;
5. predisporre apposita informativa sulle modalità d'uso degli strumenti e sui controlli;
6. definire le regole di condotta, da comunicare, che i lavoratori devono rispettare tipo la scelta del luogo dove effettuare la prestazione, l'uso del pc e di altri strumenti, l'orario di lavoro, le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro, il rispetto delle misure di sicurezza, nonché la riservatezza e la protezione dei dati aziendali, le regole per l'utilizzo della posta elettronica e di *internet*;
7. disciplinare, nell'accordo di lavoro "agile/*smart*", l'esercizio del potere di controllo sulla prestazione resa dal lavoratore all'esterno dei locali aziendali, informando i dipendenti delle modalità d'uso degli strumenti e di effettuazione dei controlli;
8. aggiornare il "*Registro delle Attività di Trattamento*" inserendo la modalità di lavoro "*smart working*";
9. predisporre apposite procedure relative a *Data Breach* che possono verificarsi in considerazione della metodologia di lavoro adottata.

È opportuno, pertanto, predisporre una sorta di "*Regolamento privacy per la modalità smart working*" che deve essere sottoscritto sia dal datore di lavoro (titolare del trattamento del dato) sia dal lavoratore dipendente (incaricato del trattamento) per accettazione.

Deve essere redatto in modo intellegibile e messo a disposizione di tutti i dipendenti attraverso la rete aziendale interna oltre che mediante affissione nelle bacheche esistenti, senza tralasciare il fatto che lo stesso deve essere periodicamente aggiornato.

Fac simile	***Smart working*** **Istruzioni trattamento per lo "*smart worker*"**

Gent.ma Sig.ra
Egr. Sig.
Via ....., n . .....
Comune ..... Prov.....

Premesso che

1. Lei è dipendente della Società _____ con sede a _____ in Via _____ Codice fiscale, partita iva e numero di iscrizione al R.I di _____;
2. Svolge la prestazione lavorativa presso la sede della società sita in _____, nei seguenti orari _____;
3. Il D.P.C.M. 10 aprile 2020 prevede che "*la modalità di lavoro agile, disciplinata dagli articoli da 18 a 23, L. 81/2017, può essere applicata dai datori di lavoro privati a ogni rapporto di lavoro subordinato, nel rispetto dei principi dettati dalle menzionate disposizioni, anche in assenza di accordi individuali previsti*";
4. Le è stata concessa la modalità di lavoro agile o "*Smart Working*" fino al termine del periodo di emergenza di cui al provvedimento del Consiglio dei Ministri del 31 gennaio 2020 e qualora lo stato di emergenza dovesse essere prolungato oltre tale termine, l'azienda Le comunicherà la proroga, con l'indicazione di una nuova data di scadenza;
5. Trascorso tale periodo verrà ripristinata, senza necessità di alcuna comunicazione preventiva, l'originaria modalità della prestazione di lavoro nei locali dell'Azienda di cui al punto 2;
6. Fermo restando che la Sua sede di lavoro ad ogni altro effetto continua ad essere presso la sede della Società come indicata al punto 1, durante il periodo in cui svolgerà l'attività lavorativa mediante modalità di lavoro agile è stabilito, su Sua espressa richiesta, che Ella operi presso il Suo domicilio sito a _____ prov. (___) in Via _____ , n. ___;
7. Le è già stata data comunicazione di nomina quale "soggetto incaricato/autorizzato" ai sensi del GDPR 2016/679 il cui contenuto è da intendersi integralmente riportato.

In ossequio alle disposizioni in materia di Privacy di cui al Regolamento Europeo n. 2016/679 e alle disposizioni nazionali (D.Lgs. 196/2003) è necessario osservare il rispetto delle seguenti

Istruzioni per il lavoro a distanza - *Smart working*

Le presenti integrano le istruzioni precedentemente date con l'attuale condizione di Smart Worker, pertanto lei avrà il dovere di:

- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- proteggere i dati contro i rischi di distruzione e/o di perdita, di accesso e/o di trattamento non autorizzato;
- rispettare e applicare il Regolamento aziendale relativo all'utilizzo degli strumenti informatici ed elettronici, all'utilizzo della posta elettronica e di internet, nonché tutte le istruzioni e misure di sicurezza;
- non violare il segreto e la riservatezza dei dati e delle informazioni trattate e/o in Suo possesso e/o disponibili sul sistema informativo aziendale;

Nella Sua attuale condizione di Smart Worker dovrà, inoltre, rispettare i seguenti obblighi:

1. individuare

- in casa una stanza o comunque uno spazio deputato per allestire la postazione di lavoro da utilizzare in modo "esclusivo" (negando, ove possibile, l'accesso ai familiari);

2. assicurarsi

- della conformità dell'impianto elettrico utilizzato per il dispositivo o i dispositivi aziendali;
- che la postazione sia sicura ovvero che non ci sia pericolo di contatto con acqua, fuoco o calore eccessivo;

3. utilizzare

- il dispositivo mobile aziendale solo ed esclusivamente per le attività lavorative a distanza, nonché gli strumenti utilizzati e i relativi sistemi operativi devono essere aggiornati all'ultima versione rilasciata;

4. spedire

- al termine di ogni giornata lavorativa un breve report sulle attività svolte (documenti consultati, documenti condivisi, colloqui con colleghi, video-call o simili intercorse con fornitori, clienti, soci o qualsiasi altro soggetto, tramite le piattaforme autorizzate, al fine di poter, eventualmente, recuperare dati e/o informazioni);

5. evitare

- di lasciare incustodita la postazione e al termine di ogni sessione lavorativa riporre tutto in luoghi ad accesso limitato (stanza chiusa a chiave oppure armadi e/o cassetti sempre chiusi a chiave);

6. comunicare

- gli orari di lavoro;
- qualsiasi anomalia riscontrata nel sistema oppure verificatasi durante l'attività.

È, inoltre, fatto assoluto divieto di:

a) salvare le credenziali di accesso su quaderni, fogli, post-it o su qualsiasi altro supporto compreso il browser; queste sono personali e riservate e devono essere custodite con la massima diligenza;

b) comunicare ai colleghi e/o a qualsiasi altra persona le proprie credenziali di accesso;

c) scaricare applicazioni/software non autorizzati;

d) disinstallare e/o disattivare il programma antivirus in dotazione; nel caso lo strumento ne fosse per qualsiasi motivo sprovvisto è obbligo del lavoratore installare l'antivirus individuato dall'amministratore di sistema dell'azienda;

e) fare uso di pennette USB o comunque basi dati esterne personali per il salvataggio dei dati, dei documenti e atti di lavoro;

f) condividere con i colleghi documenti aziendali o attività lavorative su piattaforme diverse da quella aziendale o da quella eventualmente indicata;

g) stabilire una connessione *internet* mediante il modem o la rete Wi-Fi di casa o pubblica non protette ovvero da *hot spot* sconosciuti oppure pubblici o comunque da qualsiasi altra fonte che non sia quella indicata o già impostata dall'azienda;

h) accedere a social network o a qualsiasi sito web o server mail che non appartenga a quelli già preventivamente impostati dall'amministratore di sistema;

i) comunicare con i colleghi con modalità e strumenti diversi da quelli individuati.

Tutti gli obblighi sopradescritti fanno parte integrante della prestazione lavorativa e pertanto sono da Lei dovuti in base al contratto di lavoro.

Le presenti istruzione avranno efficacia fino a quando non Le verrà revocata la modalità Smart Working.

Per quanto non previsto dalle presenti Istruzioni si rimanda alle disposizioni europee e nazionali vigenti sull'uso degli strumenti informatici in materia di protezione dei dati, nonché in materia di salute e sicurezza sul lavoro.

Luogo e data _____ FIRMA _____

(datore di lavoro)

Per ricevuta ed accettazione dell'incarico privacy per lo *smart working* (dipendente)

_____

Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Il quotidiano telematico di Euroconference
diretto da Sergio Pellegrino e Giovanni Valcarenghi
NOTIZIE E APPROFONDIMENTI
PER I PROFESSIONISTI DI TUTTA ITALIA
IscriviTi alla mailing list e
rimani informato su tutte le news
www.ecnews.it

EDITORE E PROPRIETARIO
Gruppo Euroconference Spa
Via E. Fermi, 11 - 37135 Verona

DIRETTORE RESPONSABILE
Fabio Garrini

DIREZIONE E COORDINAMENTO SCIENTIFICO
Fabio Garrini

COMITATO DI REDAZIONE
Luca Caramaschi, Sergio Pellegrino
Fabio Landuzzi, Luigi Scappini
Guido Martinelli, Giovanni Valcarenghi

COLLABORATORI ESTERNI
Andrea Bongi, Laura Mazzola
Alessandro Bonuzzi, Paolo Meneghetti
Sandro Cerato, Marco Peirolo
Luigi Ferrajoli, Leonardo Pietrobon
Alberto Alfredo Ferrario, Maurizio Tozzi
Fabio Giommoni, Francesco Zuech

REDAZIONE
Milena Martini e Chiara Ridolfi

SERVIZIO CLIENTI
Per informazioni sull'abbonamento scrivere a:
circolari@euroconference.it

SITO INTERNET
Per informazioni e ordini:
www.euroconference.it/editoria

PERIODICITÀ E DISTRIBUZIONE
Settimanale
Vendita esclusiva per abbonamento
Pubblicazione telematica

ABBONAMENTO ANNUALE 2019
Euro 220,00 Iva esclusa

I numeri arretrati sono disponibili nell'area riservata, accessibile tramite le proprie credenziali dal *link*: http://www.euroconference.it/area_riservata_login.
In caso di smarrimento delle *password* è possibile utilizzare la funzionalità "Hai dimenticato la password?" disponibile nella pagina di login.

Autorizzazione del tribunale di Verona n.1448 del 29 giugno 2001
Iscrizione ROC 13 marzo 2017 n.28049

ISSN: 2039-9618

Per i contenuti di "La circolare tributaria" Gruppo Euroconference Spa comunica di aver assolto agli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi. La violazione dei diritti dei titolari del diritto d'autore e dei diritti connessi comporta l'applicazione delle sanzioni previste dal capo III del titolo III della legge 22.04.1941 n.633 e succ. mod.
Tutti i contenuti presenti sul nostro sito *web* e nel materiale scientifico edito da Gruppo Euroconference Spa sono soggetti a *copyright*. Qualsiasi riproduzione e divulgazione e/o utilizzo anche parziale, non autorizzato espressamente da Gruppo Euroconference Spa è vietato. La violazione sarà perseguita a norma di legge. Gli autori e l'editore declinano ogni responsabilità per eventuali errori e/o inesattezze relative all'elaborazione dei contenuti presenti nelle riviste e testi editi e/o nel materiale pubblicato nelle dispense. Gli autori, pur garantendo la massima affidabilità dell'opera, non rispondono di danni derivanti dall'uso dei dati e delle notizie ivi contenute. L'editore non risponde di eventuali danni causati da involontari refusi o errori di stampa.