CORONAVIRUS
OVERCOMING THE DIFFICULTIES

COVID-19
SMART WORKING NEL RISPETTO DELLA PRIVACY

DE BERTI JACCHIA FRANCHINI FORLANI
STUDIO LEGALE

Introdotte misure per facilitare lo smartworking

Sin dalle prime fasi dell'emergenza coronavirus, il Governo ha sottolineato l'importanza dello smart working (lavoro agile) quale strumento principe per conciliare la tutela della salute dei lavoratori con l'esigenza di non fermare l'economia nazionale. In base al DPCM del 1° marzo 2020, infatti, tutti i datori di lavoro nel settore privato possono implementare lo smart working ricorrendo ad una procedura semplificata, la quale, in particolare, **non richiede la sottoscrizione di accordi individuali** con ogni singolo lavoratore (che erano obbligatori, invece, ai sensi della legge 22 maggio 2017, n. 81). Poi, il DPCM "Cura Italia" del 17 marzo 2020 ha introdotto disposizioni per promuovere l'utilizzo dello smart working anche nell'ambito della pubblica amministrazione.

Con il "Protocollo condiviso di regolazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro" del 14 marzo 2020 il Governo ha ribadito che **l'accesso ai locali aziendali deve essere ridotto per quanto possibile**, fissando alcune regole per il controllo dello stato di salute dei lavoratori, visitatori e fornitori che debbano necessariamente entrare nei locali aziendali.

Le disposizioni governative sono chiare: dove possibile, tutti devono essere messi nelle condizioni di poter lavorare da casa. Tuttavia, tale modalità di lavoro richiede una grande attenzione agli aspetti **privacy**, l'importanza dei quali, nonostante le condizioni di emergenza, non viene meno, senza dimenticare la normativa contenuta nella L. 300/1970 che disciplina il controllo a distanza dei lavoratori.

Misure di sicurezza e organizzazione del lavoro in modalità smart working

La sicurezza dei dati personali, sia "in transito" sia una volta conservati sul device utilizzato da parte del lavoratore per lo smart working, è di primaria importanza e garantirla è un obbligo dell'azienda, che sia titolare o responsabile del trattamento, imposto dal Regolamento (UE) 2016/679 ("GDPR"). L'attuazione dello smart working, in maniera repentina e inaspettata come necessario a fronte dell'attuale emergenza, soprattutto in realtà piccole e poco strutturate, potrebbe comportare seri rischi per i dati personali. Pertanto, pur tenendo conto del contesto

emergenziale e delle risorse a disposizione del datore di lavoro come previsto dall'art 32 del GDPR, l'azienda è chiamata ad adottare misure di sicurezza che siano adeguate per proteggere i dati personali del lavoratore e non solo (ad es. dati personali dei clienti che il lavoratore tratta da casa, tramite pc).

Misure organizzative

Le misure organizzative che permettono di mitigare i rischi per la privacy delle persone sono, ad esempio:

- disciplinare le modalità di utilizzo dei dispositivi aziendali e personali (se non esiste già un disciplinare aziendale in tal senso);
- definire le regole di comportamento da seguire nel luogo dove viene svolto il lavoro (eg. non allontanarsi dalla postazione di lavoro senza mettere il salvaschermo, chiudere in un armadio o cassetto dati personali in cartaceo);
- mantenere o introdurre una diversificazione degli accessi dei lavoratori ai documenti contenenti dati personali, che dovrebbero essere accessibili, anche da remoto, esclusivamente secondo le autorizzazioni rilasciate ai sensi dell'art. 29 del GDPR;
- informare i lavoratori su come evitare di cadere vittima di tecniche di phishing; è noto, infatti, che l'emergenza sia divenuta terreno fertile per hacker che stanno attaccando realtà pubbliche (es. Ministero della Sanità statunitense) e private;predisporre una procedura da seguire in caso di violazione dei dati perdonali (*data breach*), in caso di hackeraggio, furto o perdita del device ecc.).

Nel rispetto del **principio di "accountability"** o "responsabilizzazione del titolare o responsabile del trattamento" introdotto dal GDPR, è opportuno che i lavoratori siano istruiti **per iscritto** sulle misure adottate, come sopra delineate; in questo modo il datore di lavoro può dimostrare, all'occorrenza, di aver agito nel rispetto della normativa privacy applicabile.

Misure tecniche di sicurezza

Le misure organizzative devono essere affiancate da adeguate misure tecniche di sicurezza, cioè attinenti alla cybersecurity, come:

- favorire l'utilizzo di dispositivi aziendali, fornendo ai lavoratori - ove possibile - i mezzi necessari per lavorare da casa in modo da ridurre il più possibile l'utilizzo di dispositivi personali e vietando, sui dispositivi aziendali, l'uso dei social e l'accesso a siti non utili per il lavoro;
- utilizzare una connessione VPN affidabile;
- rendere disponibili tecnologie sicure per operare sui documenti necessari per l'attività lavorativa, soprattutto ove il lavoratore debba utilizzare i propri dispositivi personali;
- installare software antivirus, malware ecc… anche sui dispositivi personali dei lavoratori, ove debbano essere utilizzati per attività lavorative;
- predisporre la strumentazione necessaria per permettere al personale IT di fornire da remoto il supporto necessario ai lavoratori e di intervenire con efficacia e tempestività in caso di data breach.

Si ribadisce che, ai sensi dell'art 32 del GDPR, l'adeguatezza delle misure tecniche ed organizzative adottate può essere valutata tenendo conto dello stato emergenziale e delle risorse a disposizione del datore di lavoro.

Informazioni per il lavoratore e controlli a distanza

L'introduzione dello smart working può comportare ulteriori trattamenti di dati personali da parte dell'azienda e/o trattamenti effettuati con diverse modalità rispetto a quelli abitualmente utilizzati. L'azienda non può monitorare sistematicamente l'attività del lavoratore, pertanto è vietato usare i software aziendali e le altre tecnologie digitali per capire se lo smart worker è al pc oppure no, se sta lavorando oppure se sta compiendo attività extra lavorative.

L'uso di tali software, infatti, potrebbe costituire un controllo a distanza del lavoratore ed è consentito **esclusivamente** alle condizioni previste dalla L. 700/1970 e, in particolare, dall'art. 4 della stessa. In ogni caso, e sempre che siano soddisfatte le condizioni previste dall'art. 4, è importante, ai fini privacy, che l'azienda garantisca che:

- tali controlli siano **pertinenti e proporzionati** rispetto alla finalità perseguita ed effettuati - ove possibile considerate le circostanze - con gradualità, analizzando i dati su base aggregata e solo ove strettamente necessario compiendo controlli su base individuale, circoscrivendo in maniera ragionevole il numero dei soggetti controllati;
- i **lavoratori siano informati** in maniera dettagliata sulle modalità e le caratteristiche dei controlli, illustrando come e quando i dati vengono raccolti dai software aziendali e in quali situazioni possono essere utilizzati, fornendo tutte le informazioni richieste ai sensi dell'art. 13 del GDPR (finalità del trattamento dei dati personali, base giuridica, tempo di conservazione dei dati ecc…).

Trattamento ad alto rischio?

Infine, l'azienda deve tener presente che, in caso di utilizzo di software che comporti il controllo delle attività del lavoratore, come sopra accennato, può essere necessario, in conformità' all'art. 35 del GDPR, effettuare una valutazione dei rischi per la privacy dei lavoratori stessi. Tuttavia, considerato lo stato emergenziale e la necessità di tutelare la salute pubblica, nonché' la conseguente esigenza di ricorrere velocemente ed in modo diffuso allo smart working, una tale valutazione potrebbe essere rinviata, per essere effettuata appena possibile.

25 marzo 2020

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com

deberti jacchia