A gentile richiesta

Potrei lavorare 12 ore al giorno?

"Uno dei dottori che lavora nel nostro studio medico, è impiegato al 40%, per 8 ore al giorno su 2 giorni. Visto che ha un'altra attività anche in Italia, egli ci chiede se è possibile lavorare fino a 12 ore al giorno, facendo pausa pranzo. C'è un limite giornaliero? Potrebbe lavorare un giorno 7 ore e l'altro 9-10 ore? A livello assicurativo sarebbe consentito?"

Secondo il diritto privato e il Codice delle obbligazioni non vi sono norme che regolano la durata giornaliera o mensile del lavoro. Si prevede solo che il datore di lavoro debba concedere un giorno libero alla settimana, di regola la domenica.
Le limitazioni sulla durata sono previste dalla Legge federale sul lavoro nell'industria, nell'artigianato e nel commercio (LL, Legge sul lavoro). Sono parte integrante della protezione della salute. A tal fine esige che vi sia anche la collaborazione del datore di lavoro.
Appartenendo al diritto pubblico, la Legge sul lavoro si applica solo all'attività svolta entro i confini elvetici. Non si applica all'attività lavorativa all'estero, sebbene possano essere coinvolti un'azienda con sede legale in Svizzera o un lavoratore residente in Svizzera. Essa regola di diritto solo il lavoro prestato in Svizzera, mentre il lavoro all'estero dovrà essere svolto conformemente alle norme di quello Stato.
La Legge sul lavoro dispone che la durata massima della settimana lavorativa è di 45 o 50 ore, a dipendenza del tipo di attività e il lavoro deve essere di regola svolto tra le 06.00 e le 23.00. Al lavoratore va concesso un riposo giornaliero di almeno 11 ore consecutive tra una giornata di lavoro e la successiva.
Il lavoro giornaliero deve essere interrotto da pause che permettano al lavoratore di riposarsi e rifocillarsi e a tal fine esse devono dividere a metà il tempo di lavoro giornaliero. Il lavoro quotidiano (diurno e serale) dev'essere compreso in uno spazio di 14 ore, pause ed ore supplementari comprese. L'inizio e la fine devono situarsi entro una finestra temporale di 14 ore. Vista l'attività a tempo parziale descritta, i limiti massimi della settimana lavorativa non rischiano d'essere oltrepassati presso lo studio medico. Tuttavia, nel solco dell'obbligo di collaborazione del datore di lavoro, quando vi sono più attività a tempo parziale, le attività devono essere coordinate.
Sebbene la Legge sul lavoro non si applichi per la parte di attività all'estero, il datore di lavoro elvetico deve comunque tenerne conto per evitare che l'attività in Svizzera non possa essere considerata lesiva delle norme della Legge sul lavoro.
Qui la particolarità è data dal fatto che per l'attività in Svizzera vigono i limiti della Legge sul lavoro, che invece non si applica direttamente al lavoro svolto in Italia. Tuttavia, il datore di lavoro svizzero dovrà considerare anche l'attività effettuata in Italia per verificare che la Legge sul lavoro sia rispettata in Svizzera.
Valutando l'attività a tempo parziale per lo studio medico il lavoratore potrebbe lavorare 12 ore un giorno (con una pausa di almeno 1 ora) e altre 4 ore un altro giorno, così come potrebbe ripartire le ore svolgendone 7 un giorno e 9-10 un altro. Tale regime orario è ammissibile solo se è accertato che, considerando anche l'altra attività lavorativa, sono comunque rispettati i limiti del tempo di lavoro e di riposo.
Dal punto di vista assicurativo, posto che i parametri della Legge sul lavoro sono rispettati, non vi sono particolari problemi, essendo assicurato il suo rapporto di lavoro presso lo studio medico.

Costantino Delogu, avvocato

Tempo di lavoro: 3.2.2
Durata del lavoro: Manuale 3.2.2.1
Orario di lavoro giornaliero: Manuale 3.2.2.2

Giurisprudenza

Diritto di accesso dei sindacati al luogo di lavoro. Sentenza del Tribunale federale del 6 settembre 2017 2C_499/2015

Il Consiglio di Stato del Cantone Ticino ha regolamentato nel 2015 l'attività sindacale negli stabili amministrativi, stabilendo il principio del divieto di accesso per attività sindacali, con possibilità, previa autorizzazione, di svolgere incontri di carattere sindacale fuori dagli orari di lavoro nelle sale di riunione. Ha sottoposto a restrizioni anche l'affissione e la distribuzione di volantini e giornali periodici, possibile solo mediante consegna ai Servizi di informazione della Cancelleria dello Stato, che li avrebbe distribuiti. Il Sindacato SSP/VPOD ha ricorso contro le decisioni del Consiglio di Stato davanti al Tribunale cantonale amministrativo, senza esito, e poi davanti al Tribunale federale, dove ha ottenuto ragione. In sintesi il Sindacato contestava la conformità del regime restrittivo con la libertà sindacale e rivendicava il diritto di accedere agli stabili amministrativi per reclutare nuovi affiliati e distribuire volantini o altro materiale divulgativo.
Dopo aver esposto le norme legali che garantiscono a livello svizzero e internazionale la libertà sindacale, il Tribunale federale ha esaminato il tema del diritto di accesso dei rappresentanti sindacali agli stabili di un'azienda, sul quale la dottrina non è unanime. Per i datori di lavoro e i proprietari privati, alcune sentenze rese in ambito penale hanno negato che la libertà sindacale prevalesse sul diritto di proprietà. Il Tribunale federale ha comunque ricordato che tali sentenze si esprimevano solo su casi concreti, relativi a condanne penali, e che non vi era ancora una decisione di principio sul tema di sapere se la libertà sindacale poteva prevalere sul diritto di proprietà e garantire il diritto di accesso dei rappresentanti sindacali a un luogo di lavoro privato. Nel caso concreto, tuttavia, lo Stato era datore di lavoro e proprietario del luogo di lavoro. Il Tribunale federale ha pertanto lasciato indeciso il quesito di sapere se i rappresentanti sindacali hanno un diritto di accesso alla proprietà privata in virtù della libertà sindacale. In effetti, quando lo Stato è datore di lavoro e proprietario del luogo di lavoro, la libertà sindacale comprende come componente essenziale il diritto dei rappresentanti sindacali di accedere agli immobili statali per esercitare le attività necessarie all'operatività del sindacato. I rappresentanti sindacali hanno pertanto un diritto di accesso agli stabili statali, che non è assoluto e le cui modalità vanno concordate con il datore di lavoro pubblico. Il Tribunale federale ha ritenuto che la regolamentazione emanata dal Consiglio di Stato era una limitazione grave della libertà sindacale. Lo Stato può regolamentare l'accesso dei rappresentanti sindacali ai suoi stabili, ma non può stabilire un divieto di principio, anche se con possibilità di deroghe, né un sistema di autorizzazione tale da rendere difficile l'accesso.

Emanuela Colombo Epiney, già giudice al Tribunale d'appello del Cantone Ticino

La posizione dei sindacati rispetto all'azienda: Manuale 3.11.1
Sindacati: diritto all'informazione: Manuale 8.5

IMPRESSUM

NewsletterLavoro è la pubblicazione mensile del sistema d'informazione **Il diritto del lavoro applicato**.
Editore: Robert Boss
Responsabile Newsletter: Elisabetta Bacchetta
Hanno collaborato: Gianni Cattaneo, Carlo Del Bo, Sharon Guggiari Salari, Costantino Delogu, Emanuela Colombo Epiney.
Boss Editore SA - CH 6997 Sessa
tel. +41(0)91 600 93 03

Redazione: *lisa.bacchetta@boss-editore.ch*
Amministrazione: *info@boss-editore.ch*

BOSS conoscenza applicata

NEWSLETTER LAVORO

Maggio 2018

Editoriale

Questa edizione della Newsletter Lavoro è dedicata al GDPR. Dietro queste quattro lettere si cela un cambiamento radicale nella gestione dei dati personali. Stiamo parlando infatti del nuovo regolamento europeo sulla protezione dei dati personali che entra ufficialmente in vigore il 25 maggio 2018. Grazie ai competenti e approfonditi interventi di Gianni Cattaneo, Carlo Del Bo e Sharon Guggiari Salari, continuando nella lettura e in pochi minuti avrete una visione d'insieme piuttosto completa di questa tematica che, ce lo dicono gli esperti, avrà un notevole impatto nella quotidianità di molte aziende.
Con la rubrica "A gentile richiesta" il nostro esperto risponde alle domande di uno studio medico che ha tra i suoi dipendenti un dottore impiegato a tempo parziale che esercita la professione anche presso una struttura sanitaria in Italia. Il dipendente chiede allo studio medico di poter concentrare il suo tempo parziale presso di loro, lavorando fino a 12 ore al giorno.
Con la rubrica Giurisprudenza la nostra esperta fa chiarezza su una questione alla base di tensioni tra datori di lavoro e sindacati: a questi ultimi può essere vietato di principio l'accesso ai luoghi di lavoro? Secondo il Tribunale federale un tale divieto generalizzato non è ammesso in quanto limiterebbe in maniera grave la libertà sindacale. La massima istanza ha così accolto il ricorso di un sindacato ticinese. Ne consegue che i rappresentanti sindacali hanno di principio un diritto di accesso agli stabili statali, e che dovranno accordarsi con il datore di lavoro pubblico sulle modalità con cui esercitare tale diritto.

Elisabetta Bacchetta

All'interno:

GDPR: le ripercussioni del nuovo regolamento

Protezione dei dati: si cambia musica

Intervista a Gianni Cattaneo, avvocato specializzato in diritto informatico

Questa edizione della Newsletter Lavoro è dedicata al nuovo regolamento europeo sulla protezione dei dati personali (GDPR). Nella prima intervista Gianni Cattaneo ci offre una panoramica di quali saranno le concrete ripercussioni per le aziende svizzere e ticinesi.
Il regolamento europeo (GDPR) entrerà in vigore il 25 maggio 2018 nei Paesi facenti parte dell'Unione Europea. Quali ripercussioni vi saranno per le aziende svizzere e ticinesi?
L'impatto, dal profilo giuridico, è assai rilevante. Pochi imprenditori e amministratori ne sono tuttavia coscienti. Le cose si stanno per fortuna muovendo, grazie soprattutto alle iniziative promosse da vari enti ed associazioni che rappresentano gli interessi dei settori dell'economia maggiormente toccati.

Quali aziende avranno maggiori ripercussioni dall'entrata in vigore del nuovo regolamento europeo sulla protezione della privacy?
Le aziende più toccate sono quelle attive nella fornitura di beni e servizi a persone fisiche localizzate nell'UE, le aziende che utilizzano strumenti di monitoraggio del comportamento di persone nell'UE (ad esempio attraverso cookies, newsletter, siti web ecc.) e quelle che detengono un'organizzazione stabile nell'UE, come una succursale, una filiale o un rappresentante. Un'altra categoria che sarà particolarmente toccata: le imprese che trattano dati per conto di aziende europee (ad esempio: hosting, SaaS, PaaS ecc.) e quelle che trattano dati congiuntamente ad aziende europee: in questi casi, le aziende europee, posto che esse avranno l'obbligo di delegare il trattamento di dati solo a soggetti "GDRP compliant", esigeranno dai provider svizzeri la conferma della conformità alle norme europee, pena la revoca immediata degli incarichi.
Quali sono i cambiamenti più importanti relativi alla protezione dei dati introdotti dal nuovo regolamento?
Le aziende devono ripensare la propria organizzazione creando un ecosistema rispettoso e in grado di reagire rapidamente alle richieste delle parti interessate, nonché alle violazioni della sicurezza. Il GDPR impone di operare secondo determinati principi, tra cui quello di minimizzazione dei trattamenti, che richiede di trattare solo i dati strettamente necessari, concedere una serie di diritti, in particolare i diritti di accesso e portabilità dei dati, informare compiutamente sui trattamenti effettuati, quando necessario, acquisire un consenso libero, specifico, esplicito ed inequivocabile ai trattamenti di dati, formalizzare i rapporti con i data processor, implementare sistemi informatici sicuri e in grado di reagire rapidamente alle violazioni della sicurezza, ad esempio in caso di furti di dati.
A certe condizioni (piuttosto severe), effettuare una valutazione d'impatto sui trattamenti di dati, tenere un registro dei trattamenti e nominare un responsabile del trattamenti di dati (DPO, Data Protection Officer) e a certe condizioni, nominare un rappresentante nell'UE per gestire in contatti con le autorità.
Qual è la sua opinione riguardo al nuovo regolamen- *segue a pag. 2→*

segue da pag. 1→

Protezione dei dati: si cambia musica

to? Ritiene vi sia un miglioramento nella protezione dei dati e perché?
Il GDPR rivoluziona la protezione dei dati in maniera estremamente positiva. Da una parte responsabilizza le aziende e, dall'altra, crea diritti e meccanismi al beneficio delle parti interessate per giungere finalmente ad una protezione effettiva dei dati personali.
Qual è il suo consiglio alle aziende ticinesi per affrontare al meglio questo cambiamento?
Le aziende devono innanzitutto "mappare" i trattamenti di dati personali, chiedendosi: Quali dati tratto? Per quali motivi? Chi ha accesso ai dati? Da dove provengono i dati? Con chi condivido i dati? Per quanto tempo conservo i dati? Quali informazioni comunico agli interessati? Come è organizzata la mia piattaforma informatica? Quali attività svolgo online, ad esempio nel settore commerciale e marketing/pubblicitario? L'azienda ticinese deve valutare con uno specialista se essa rientra o meno nel campo di applicazione del GDPR oppure se il GDPR si applica indirettamente, in quanto l'azienda rientra nella "filiera" internazionale del trattamento di dati. In caso affermativo, va iniziato al più presto il processo di valutazione dello stato di fatto e la messa a norma. A livello di priorità, ritengo che il sito web debba essere messo in regola con la massima urgenza, così come la formalizzazione di eventuali nomine a responsabili del trattamento dati di provider europei.
In quali casi sono previste sanzioni? Che tipo di sanzioni verranno applicate?
Le sanzioni, sulla carta, sono elevatissime e giungono fino al 4% del fatturato mondiale, rispettivamente a 20 milioni di euro. Vi potranno essere anche ulteriori sanzioni a livello dei singoli Stati, in particolare di natura penale.
Quali sono le autorità che vegliano in Europa sull'applicazione del regolamento? E in Svizzera?
Nell'UE ogni Stato possiede una propria Autorità garante. In Svizzera, tale ruolo è affidato all'Incaricato federale per la protezione dei dati.
Non teme che la Svizzera diventi un Paese eldorado per il trattamento illegale di dati personali?
Non lo credo assolutamente, per il semplice fatto che il GDPR ha considerato tale rischio e propugna un regime di protezione dei dati a carattere extra-territoriale, slegato dal concetto di ubicazione fisica del trattamento di dati.
Ritiene che la Svizzera si adeguerà al regolamento europeo e in che modo?
La Svizzera deve provvedere all'armonizzazione del proprio diritto interno, sia pubblico, sia privato, onde poter mantenere la libera circolazione dei dati personali con l'UE. Coerentemente, ancorché i tempi si siano di recente "pericolosamente" dilatati, è in corso la revisione della legge federale sulla protezione dei dati, che riprenderà la sostanza del GDPR. In altre parole, le aziende svizzere che si stanno muovendo per implementare il GDPR, non solo stanno riducendo i propri rischi legali nei confronti dell'UE e implementando un sistema rispettoso dei diritti dei propri utenti e clienti, bensì stanno anticipando un "percorso" ineluttabile anche dal profilo del (futuro) diritto interno.

Nuove norme sulla protezione dei dati: Manuale 3.2.6.3.3

Gianni Cattaneo

Gianni Cattaneo è avvocato e notaio. Dal 2016 è membro della Commissione cantonale della protezione dei dati e dal 2008 arbitro internazionale Swiss Chambers Arbitration Institution. Insegna diritto informatico e di internet presso diversi istituti, tra cui Supsi, Franklin University Switzerland e Centro Studi Bancari di Vezia. Tra le sue pubblicazioni: "L'azienda svizzera e i cookies", "Genitori nella rete" e "I delitti contro l'onore commessi online".

Pensi che il GDPR non si applichi alla tua azienda? Potresti sbagliarti.
Sei un'azienda che ha il sito internet in inglese? Sul tuo sito internet appare il numero di telefono con il prefisso internazionale (+41)? Dal sito risulta chiaramente che offri beni e/o servizi alla clientela italiana o più in generale alla clientela europea? Hai un sito internet che utilizza google analytics oppure dei cookies? Mandi newsletters a persone dell'UE?

Gli esempi citati sopra sono solo alcuni dei casi concreti in cui vi è il forte rischio che il GDPR si applichi ad aziende svizzere. Esso può dunque concretamente coinvolgere banche, fiduciarie, studi legali, cliniche, negozi, ecc.
Il GDPR ha infatti una portata extraterritoriale e si applica a tutte le persone/aziende svizzere che offrono beni e/o prestazioni di servizio a interessati che si trovano nell'Unione Europea (UE) oppure monitorano il comportamento delle persone all'interno dell'UE (articolo 3 /2 GDPR).

In sostanza il GDPR rafforza i diritti delle persone fisiche dell'UE di controllare i propri dati a carattere personale. Le imprese devono dunque adattare le loro misure di protezione dei dati.

Tra le novità più importanti che il GDPR introduce, rispetto alla nostra attuale legislazione svizzera in materia protezione dati, si possono citare:
- la portabilità dei dati: l'interessato (a determinate condizioni) ha il diritto di ricevere i dati personali che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico (es: chiavetta USB) e di trasmettere tali dati a terzi,
- l'obbligo, per chi offre beni/servizi in EU e che tratta dati sensibili su larga scala di nominare un rappresentante nell'UE,
- le elevatissime sanzioni amministrative.

Da un punto di vista strategico, in vista dell'entrata in vigore del GDPR, il consiglio alle aziende è di valutare se in termini di fatturato conviene o meno offrire i propri/beni servizi a persone dell'UE e, se tale è il caso, d'iniziare i processi necessari per adeguarsi al GDPR. Sul sito internet di Economiesuisse (www.economiesuisse.ch/it/datenschutz-online-check) si può trovare un test on line per verificare l'applicabilità del GDPR e le misure concrete da adottare.

Sharon Guggiari Salari, Avvocato specialista FSA diritto del lavoro

Tutte le edizioni di *NewsletterLavoro* sono consultabili nell'area riservata ai clienti sul sito: ***www.boss-editore.ch***.
Diversi indici facilitano la ricerca per parola chiave.

Gli attacchi aumenteranno

Abbiamo incontrato Carlo Del Bo, esperto di cybersecurity

Il nuovo regolamento europeo per la protezione dei dati è un passo avanti?
È un cambiamento positivo e radicale nella gestione della privacy. Finalmente vi è una regolamentazione della protezione dei dati personali. Il suo principio cardine è che i dati personali devono essere costantemente monitorati e in caso di data bridge, ossia in presenza di una violazione dall'esterno o dall'interno, vi è l'obbligo di notificarla alle autorità entro 72 ore.
Quali sono le aziende maggiormente a rischio di attacchi informatici?
Tutte, ma soprattutto le aziende che dispongono di un'ampia varietà di dati personali, come, ad esempio, gli ospedali e le case di cura. Queste strutture possiedono sia i dati relativi alle carte di credito che le schede dei pazienti come pure i dati personali.
Come possiamo immaginarci il futuro della sicurezza informatica?
Una cosa è certa: gli attacchi informatici aumenteranno. Non dobbiamo chiederci dunque se avverranno, ma quando. Nel mio lavoro eseguo spesso dei "vulnerability assessment" nei quali simuliamo un attacco a un'azienda per mettere alla prova la vulnerabilità della sua rete. Un programmatore o un ingegnere informatico, in ogni caso un tecnico, si cala nei panni di un hacker e cerca di entrare in un sistema informatico. L'azienda in genere non si accorge neppure che qualcuno è entrato nel suo sistema.
Quali misure concrete possono mettere in atto le aziende per proteggersi dagli attacchi informatici?
Il primo passo è fare un inventario, una mappatura, dei dati sensibili che l'azienda tratta. Mi riferisco ai dati personali relativi a collaboratori, clienti e fornitori. Va valutato il flusso delle informazioni, tenendo conto anche di ciò che accade al di fuori del perimetro aziendale. Pensiamo alla documentazione aziendale in possesso di un avvocato. Inoltre non va dimenticato che i dati sensibili non sono archiviati solo su supporti informatici, ma anche cartacei. Se metto in sicurezza la mia rete informatica, dovrò fare lo stesso fisicamente chiudendo a chiave la porta dell'archivio cartaceo. Terminato questo assessment, dovrà essere messo a punto un remediation plan che contenga le misure di messa in sicurezza unitamente a un supporto strategico per la mitigazione dei rischi. Ricordo inoltro che il GDPR impone il monitoraggio costante della tutela dei dati personali.
Sicurezza informatica e cybersecurity sono sinonimi?
Non confondiamo i termini. Con sicurezza informatica intendiamo l'insieme dei dispositivi che vanno installati in un sistema per ridurre il rischio di subire intrusioni dall'esterno. La cybersecurity è invece quel settore che studia l'impatto che il rischio informatico ha sul business. A questo livello si lavora maggiormente impostando determinate scelte strategiche. Per semplificare potremmo paragonare la cybersecurity alla criminologia e la sicurezza informatica alla polizia.
La Svizzera si adeguerà al GDPR?
Questa rivoluzione in atto nella protezione dei dati personali è un fiume in piena che non potrà essere deviato ai confini nazionali elvetici. La legislazione svizzera si avvicinerà alle linee guida del GDPR, anche se attualmente ci troviamo effettivamente in una sorta di limbo.
L'applicazione del GDPR sarà un onere importante per le aziende?
Non sarà certamente un'operazione a costo zero. Ma d'altro canto sono previste sanzioni importanti per chi contravviene il regolamento. A mio parere qui vi è anche una grande occasione di refresh per le aziende che potrebbero sfruttare le misure di protezione dei dati messe in atto come strumento di marketing. Ad oggi non esiste ancora una "certificazione GDPR" ma posso immaginare che in futuro vi saranno aziende che potranno fregiarsi di qualcosa di simile. Ma non mi limiterei solo a questi aspetti. Basti pensare ai settori Ricerca e sviluppo delle aziende che godranno anch'essi di una maggiore protezione rispetto allo spionaggio industriale.
L'introduzione del GDPR comporterà la creazione di nuovi posti di lavoro?
Sì e qui vedo un'ulteriore occasione di crescita. Nelle grandi aziende saranno create posizioni per DPO, Data Protection Officer, professionisti responsabili della sicurezza informatica che dovranno rendere conto direttamente alla direzione aziendale.

Carlo Del Bo

Carlo Del Bo è International Security Advisor per diverse multinazionali italiane ed estere. Laureatosi alla Criminal Justice dell'Università Northeastern University di Boston con una tesi su "Computer Crime", ha conseguito un Master in Security Management all'Università Bocconi e un Master in Business Intelligence. Dal 2017 è Executive Advisor di Gruppo Sicurezza SA, società di servizi e consulenza con sede a Savosa e specializzata in Security e Risk Management dove si occupa di Cyber, Crisis Management, Risk Assessment e consulenza internazionale.

I prossimi seminari di Boss Editore

"Lavoratori distaccati a 360°"
17.05.2018

"Notifiche e permessi di lavoro"
5.06.2018

Maggiori info:
www.boss-editore.ch
Seminari 2018

Attacchi informatici

Malware: indica un vasta categoria di codici nocivi quali virus, worm e cavalli di troia.
Phishing: è una metodologia di attacco che simula nella grafia e nel contenuto una comunicazione ufficiale e conosciuta.
DoS o DDoS: è una tipologia di attacco che ha lo scopo di saturare deliberatamente le risorse di un sistema informatico e bloccarlo.
Sql Injection: è una metodologia piu' complessa usata per attaccare i server che contengono informazioni di valore quali password-users o dati sensibili.
Man in the middle: di fatto "uomo nel mezzo" ovvero un attaccante che si inserisce nel traffico dati di due utenti e fa credere ad entrambe le parti che stiano interagendo tra loro.
Glossario a cura di Carlo Del Bo