AZIENDA OSPEDALIERO - UNIVERSITARIA
Città della Salute e della Scienza di Torino

ALLEGATO 3)
AL REGOLAMENTO

ISTRUZIONI SU PROTEZIONE DEI DATI PERSONALI

PER AUTORIZZATI AL LAVORO AGILE (SMART WORKING)

1 Premessa

In occasione dell'avvio della modalità lavorativa in smart working o lavoro agile, si ricorda che è doveroso prestare costante attenzione alla protezione dei dati personali e adottare, in qualsiasi occasione, lavorativa e privata, un comportamento improntato alla difesa della privacy degli interessati che entrano in relazione con l'Azienda.
A tal fine si richiamano i contenuti delle informazioni fornite ex artt. 13 e 14 Regolamento UE 2016/679 del 27 aprile 2016 e norme di armonizzazione per il trattamento dei dati personali e categorie di dati personali dei dipendenti, nonché le Policy dell'Azienda in materia, con le obbligazioni ivi riportate a carico dei singoli dipendenti, in relazione al ruolo ricoperto nel sistema privacy aziendale e in ottemperanza al principio dell'accountability (responsabilizzazione) previsto dal sopraccitato Regolamento.

2 Smart working

Lo smart working o lavoro agile (art.18, Legge 22.05.2017, n. 81) è una "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".
L'esecuzione della prestazione lavorativa all'esterno della sede aziendale impone la massima attenzione sui temi della riservatezza e presuppone che il/la dipendente rimanga sempre concentrato sulle modalità di lavoro, al fine di svolgere la propria attività anche al di fuori di una postazione fissa, in modo corretto ed idoneo per proteggere l'operatività e la reputazione dell'Azienda.

In particolare:
1) Il/la dipendente dovrà aver cura di svolgere la prestazione lavorativa in ambienti tali da consentire comunicazioni stabili, efficienti e non disturbate da rumori circostanti.

2) Le conversazioni tra il/la dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto è obbligo del/della dipendente:

- evitare di pronunciare ad alta voce dati riservati/personali, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- accertarsi che i congiunti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa, o in subordine garantiscano la medesima segretezza alla quale è tenuto il dipendente pubblico;
- non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;
- nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione,

- non è consentito comunicare dati personali o sanitari agli organi di stampa, le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'Addetto Stampa Aziendale.

L'Azienda, in qualità di Titolare, stabilisce che, ai sensi dell'art. 24 comma 1 del Regolamento U.E. 2016/679, la documentazione inerente all'attività lavorativa dovrà risiedere preferibilmente sulle cartelle di rete, osservando le indicazioni previste nelle circolari della S.C. IT prot.0041141 del 17.04.2019 e prot. 0063439 del 21.06.2019 (ad es. cifrando i dati personali).

Fermo restando che le Strutture debbono adottare modalità di lavoro esclusivamente immateriali, nella transizione il/la dipendente deve prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) sistemi e documenti contenenti dati personali.

Per quanto riguarda la generica conservazione dei dati personali utilizzati dal/dalla dipendente in smart working, il Responsabile della Struttura deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal/dalla dipendente; il lavoro in modalità smart working non dovrà essere effettuato al di fuori di ambienti privati protetti che garantiscano la necessaria riservatezza della prestazione.

Più in dettaglio, per quanto concerne l'uso assolutamente residuale di mezzi materiali, l'utilizzo di documenti cartacei contenenti dati personali e prelevati dagli archivi dell'Azienda, il trasferimento di dati personali all'esterno deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi della società; la circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile; i dati devono essere raccolti in porta documenti riportanti l'identificazione del/della dipendente utilizzatore, dell'Azienda e il suo recapito telefonico.

In particolare i documenti cartacei:

- devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi collocati negli archivi aziendali dedicati alla loro conservazione;
- non devono essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge lo smart working è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possono essere visionati da persone non autorizzate;
- devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili).

Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le indicazioni fornite dall'Azienda all'atto dell'autorizzazione al trattamento dei dati e si ribadisce quanto già prescritto dalle Policy dell'Azienda in materia di Privacy e in particolare:

- la password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della dipendente, che altri ne vengano a conoscenza;
- non deve essere utilizzata la mail aziendale o la password aziendale per la registrazione su altri siti internet;
- il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni in modalità smart working (P.C., smartphone, ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate; in caso di allontanamento anche temporaneo dalla postazione di lavoro il/la dipendente è tenuto a disconnettere la sessione di lavoro bloccando

l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo);
- i personal computer utilizzati per lo svolgimento dell'attività lavorativa in modalità agile ,devono essere utilizzati preferibilmente in modo esclusivo dall'utente o, in caso di uso promiscuo, in modo da consentire l'accesso con utenze separate ;
- non devono essere utilizzati dispositivi di memorizzazione esterna (come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al regolamento).
- la trasmissione di dati mediante mail deve avvenire secondo le istruzioni già impartite, cioè all'interno dell'Azienda ("Comunica") ovvero se all'esterno previa cifratura (megallegati) del documento qualora contenga dati personali.

I trattamenti effettuati dal/dalla dipendente devono rispettare il principio di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti, come da istruzioni fornite in punto all'atto dell'autorizzazione dell'Azienda al trattamento dati.

Nell'ambito delle proprie attività e in osservanza alle misure derivanti dal sistema procedurale, l'Azienda per garantire la sicurezza dei dati personali, tratta dati:

- esatti e, se necessario, aggiornati;
- archiviati in una forma che consenta l'esercizio dei diritti da parte dell'interessato di cui al Capo III del Regolamento Europeo;
- conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- ove necessario e compatibile, anonimizzati, pseudonimizzati o cifrati.

Il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato) nell'eventuale trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);

E' fondamentale sottolineare che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Tale violazione può afferire a una "violazione della riservatezza", in caso di divulgazione o accesso accidentale ai dati personali, alla "perdita della disponibilità"(comprese le ipotesi di sottrazione e/o furto), in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.

La violazione, in rapporto alla sua gravità, può comportare per l'Azienda la Notifica del Data Breach, cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.

A tal fine si ribadisce l'obbligo del/della dipendente di segnalare qualunque ipotesi di violazione dei dati personali (a mero titolo esemplificativo: perdita, distruzione, divulgazione), al Responsabile della struttura preposto (Delegato al trattamento) e al Responsabile della Protezione dei Dati(DPO), tempestivamente e, comunque, nei termini e con le modalità previste dalla procedura aziendale approvata con deliberazione del Direttore Generale n. 956/2019 del 11/07/2019 reperibile nell'Intranet Aziendale : Privacy/Data Breach, anche al fine di consentire il rispetto dei ristretti termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.

E' obbligazione contrattuale del/della dipendente rispettare le suddette istruzioni e in caso di violazione ne consegue la responsabilità prevista dalla normativa vigente in materia.