Allegato AUTORIZZAZIONE PERSONALE VACCINAZIONI COVID 19

ADDENDUM PRIVACY
PROTEZIONE DEI DATI PERSONALI

In occasione della sua partecipazione all'attività vaccinale COVID 19 per conto di ASL 3, Le ricordiamo che è necessario 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 si relazionano con l'Ente.

A tal fine si richiamano i contenuti delle informazioni fornite ex artt. 13 e 14 Regolamento Unione Europea 679/2016 del 27 aprile 2016 e norme di armonizzazione per il trattamento dei dati personali e categorie di dati personali dei dipendenti, nonché della normativa interna dell'Ente in materia, con le obbligazioni ivi riportate a carico dei singoli soggetti che collaborano con ASL 3 in relazione al ruolo ricoperto e in ottemperanza al principio dell'accountability (responsabilizzazione) previsto dal sopraccitato Regolamento, come anche consultabili, nelle sezioni dedicate, sulla intranet di Asl3 (normativa/privacy) e sul sito internet di Asl3 www.asl3.liguria.it (politica della privacy aziendale). Si vedano in particolare il DPS (Documento Programmatico sulla Sicurezza) vigente in Asl3.

Inoltre si riportano due documenti: "Cinque Comportamenti Fondamentali" e "Decalogo Privacy, che hanno la finalità di ulteriormente orientare gli atteggiamenti e i comportamenti dei collaboratori che espletano detta attività.

"Cinque comportamenti fondamentali"

Riservatezza: proteggi le informazioni riguardanti il tuo lavoro e l'azienda con cui collabori. Non condividere con terzi dati, idee, soluzioni, opinioni che riguardano la tua attività lavorativa, potresti danneggiare il tuo lavoro e anche il tuo interlocutore;
Attenzione: resta concentrato sull'attività lavorativa ovunque tu sia: sui documenti, sui file, sugli strumenti di lavoro; la distrazione può facilmente provocare smarrimenti, diffusione di informazione a soggetti non autorizzati, errori operativi che possono danneggiare i dati personali, i loro interessati e le aziende titolari dei dati stessi;
Precisione: l'accuratezza nel fare le cose ti consente di lavorare in modo efficace ed efficiente anche al di fuori del contesto di ASL3. Cura con scrupolosità le conversazioni, l'invio della mail, il salvataggio dei dati nel repository aziendale, evita il ricovero temporaneo di documenti in archivi estranei al perimetro aziendale abituale;
Ordine: la sistematica e schematica organizzazione delle risorse e degli strumenti di lavoro previene disguidi difficili da risolvere quando sei fuori dalla tradizionale sede di lavoro. Ogni cosa, ogni file, ogni mezzo devono avere collocazioni e utilizzi abituali e sperimentati;
Separatezza: tieni separata la tua vita lavorativa dalla tua sfera privata, familiare e sociale. In questo modo proteggi anche i tuoi familiari e i tuoi amici. Infatti, ogni interferenza può provocare irregolarità o comportamenti non corretti, che dovranno essere oggetto di riparazione, con dispersione di energie e risorse da parte Tua, della Società e dei terzi coinvolti.

"Decalogo Privacy"

Il Lavoro esterno ad ASL 3 impone la massima attenzione sui temi della riservatezza e presuppone che il/la collaboratore rimanga sempre concentrato sulle modalità di lavoro, al fine di svolgere la propria attività in modo corretto ed idoneo per proteggere l'operatività e la reputazione dell'Ente.

In particolare detta attività non dovrà essere effettuata, a tal fine, al di fuori di ambienti protetti, che garantiscano la necessaria riservatezza della prestazione e/o connettendosi con collegamenti WIFI a reti aperte.

1) Le conversazioni tra il/la collaboratore 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 collaboratore:

- Evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- Accertarsi che terzi non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;
- Non utilizzare terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;

- Nel caso di conversazioni telefoniche instaurate in 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;

2) L'Ente, 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 esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al Regolamento.

3) Il/La collaboratore deve evitare di trasportare e comunque 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) documenti contenenti dati personali.

4) Per quanto riguarda la generica conservazione dei dati personali utilizzati dal/dalla collaboratore il Responsabile dell'unità organizzativa di afferenza deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente esterno ad ASL 3 utilizzato dal/dalla collaboratore. L'attività svolta non dovrà essere effettuata, a tal fine al di fuori di ambienti protetti, che garantiscano la necessaria riservatezza della prestazione.

5) Più in dettaglio per quanto concerne l'utilizzo di eventuali documenti cartacei contenti dati personali e prelevati dagli archivi dell'Ente, si sottolinea che il trasferimento di dati personali all'esterno di ASL 3 deve essere evitato e comunque giustificato da necessità strettamente correlate all'esercizio dell'attività, agli obblighi di legge o alla difesa degli interessi di ASL 3. 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 collaboratore utilizzatore e il suo recapito telefonico.

In particolare i documenti cartacei:

- devono essere utilizzati solo per il tempo necessari allo svolgimento dei compiti assegnati e poi ripartiti 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 l'attività 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).

6) Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le indicazioni fornite in punto all'atto dell'autorizzazione al trattamento dati dall'Ente e si ribadisce quanto prescritto dal DPS ASL 3 vigente e dal regolamento ASL3 relativo al trattamento dati mediante strumenti elettronici adottato con deliberazione n 433/2018 e aggiornato con determinazione dirigenziale n. 62/2019 che individuano, tra l'altro, le misure di sicurezza da adottare in caso di utilizzazione di strumenti BYOD e in particolare:

- La password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della collaboratore, che altri ne vengano a conoscenza;
- Il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni (P.C., smartphone, personali e/o aziendali ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il/la collaboratore 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).
- 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.

7) I trattamenti effettuati dal/dalla collaboratore 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 al trattamento dati dell'Ente.

8) Nell'ambito delle proprie attività e in osservanza alle misure derivanti dal sistema procedurale, gestionale e tecnico instaurato dall'Ente per garantire la sicurezza dei dati personali, il collaboratore 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 collaboratore 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);

9) 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'Ente 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 collaboratore di segnalare qualunque ipotesi di violazione dei dati personali al responsabile della struttura preposto e al Responsabile della Protezione dei Dati di ASL 3, tempestivamente e, comunque, nei termini previsti dalla normativa interna aziendale in materia, 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.

10) Il/La collaboratore sarà specificatamente autorizzato al trattamento, informato/a e formato/a dal Titolare in merito alle peculiarità del trattamento dei dati personali conseguenti alla Sua attività ed ai conseguenti rischi e misure di sicurezza adottate e da adottarsi, che integrano quelle fornite all'atto dell'autorizzazione ai trattamenti di competenza, in relazione al ruolo ricoperto per conto dell'Ente.
E' obbligazione del/della collaboratore rispettare dette istruzioni e partecipare alle attività formative previste dell'Ente in punto.

11) Il/La collaboratore è consapevole ed accetta che ASL3 verifichi il rispetto delle misure di sicurezza informatiche ed operative che Gli/Le sono state indicate all'atto dell'autorizzazione all'attività, nel rispetto delle previsioni della normativa vigente in materia e dell'art.4 della L.300/70 e s.m.i..

Per ricevuta e accettazione
Il collaboratore esterno

Data

_____ _____