REPUBBLICA ITALIANA
Regione Siciliana

ASSESSORATO DELLA SALUTE
Dipartimento Regionale per le Attività Sanitarie e Osservatorio Epidemiologico

Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza dell'Amministrazione

Il trattamento dei dati personali effettuato per conto dell'Amministrazione dovrà avvenire nel rispetto dei principi del Regolamento UE 2016/679, del Dlgs 101/2018 e delle altre disposizioni vigenti in materia.

Per trattamento di dati personali si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Il trattamento dei dati per conto dell'Amministrazione può avvenire nei seguenti casi:

- sia previsto da obblighi di legge cui è soggetta l'Amministrazione;
- riguardi l'interesse pubblico o esercizio di pubblici poteri propri dell'Amministrazione;
- sia necessario per l'adempimento di obblighi contrattuali stipulati dall'Amministrazione;
- sia necessario a garantire gli interessi vitali della persona interessata o di terzi;
- l'interessato abbia espresso il consenso esplicito in favore dell'Amministrazione;
- sia necessario per tutelare interesse legittimo prevalente dell'Amministrazione o di terzi cui i dati vengono comunicati.

Il trattamento dei dati avviene mediante documentazione cartacea, strumenti informatici e telematici, con modalità strettamente correlate alle finalità stesse e comunque in modo da garantire la sicurezza e la riservatezza adeguata.

Nel trattamento dei dati personali va osservato il principio di pertinenza e di non eccedenza, limitando i dati trattati a quelli strettamente necessari ed attinenti al compito da svolgere. È pertanto vietato accedere a dati personali non necessari al compito amministrativo che deve svolgersi.

I dati personali debbono essere trattati per le finalità istituzionali dell'Amministrazione secondo le modalità di cui alle presenti istruzioni e di ogni ulteriore specifica disposizione in merito emessa dal Titolare dei trattamenti di dati personali - Assessore della Salute pro-tempore, dal Responsabile del trattamento – Dirigente Generale pro-tempore del Dipartimento per le Attività Sanitarie ed Osservatorio Epidemiologico, incaricato dal Titolare, e dal sub- Responsabile, il dirigente della struttura intermedia o dell'unità operativa incaricato dal Responsabile o dal Titolare, nell'ambito delle rispettive competenze e prerogative.

Il trattamento dei dati personali, che rientri nei suddetti casi consentiti, potrà essere effettuato da:

1) il personale che agisce per conto dell'Amministrazione, nell'ambito dei compiti assegnati;
2) le società, gli enti, i consorzi che forniscono specifici servizi all'Amministrazione o che svolgono attività connesse, strumentali o di supporto a quelle dell'Amministrazione stessa purché designati a svolgere la funzione di sub-Responsabile tecnico. Tali soggetti dovranno essere stati appositamente ed esplicitamente autorizzati dal Titolare, o dal Responsabile o dal sub-Responsabile (qualora autorizzato dal Responsabile)
3) i soggetti a cui la facoltà di accedere ai dati personali sia riconosciuta da disposizioni di legge o di normativa comunitaria.

L'accesso ai dati è consentito nella misura strettamente necessaria ad adempiere ai compiti assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata.

In particolare i soggetti autorizzati che trattano i dati per conto dell'Amministrazione osserveranno almeno le seguenti misure di sicurezza, compatibilmente con gli arredi disponibili nella Struttura in cui essi prestano servizio:

- è vietato comunicare a persone non autorizzate i dati personali di qualunque genere (giudiziari, sanitari o altri dati), elementi e informazioni dei quali il soggetto autorizzato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni. In caso di dubbio, è necessario accertarsi che la persona a cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio dirigente;
- è vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base o altro, se non previa richiesta formale di accesso agli atti;
- la documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati personali, al termine dell'orario di lavoro, saranno riposti in cartelle ed armadi chiusi in modo da evitare che, in assenza degli autorizzati i soggetti non autorizzati ne possano prendere visione;
- qualora i documenti contengano dati sensibili o giudiziari essi saranno riposti in archivio ad accesso controllato. I documenti contenenti dati sanitari, anche se pervenuti senza busta, saranno conservati in buste chiuse ed in armadi chiusi e, se trasmessi, andranno inseriti in buste chiuse con lettera di accompagnamento da cui non si evincano i dati sanitari in essa contenuti;
- per quanto riguarda i flussi di documenti cartacei all'interno degli uffici regionali, saranno adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in cartelle, carpette o buste chiuse ecc.);
- l'accesso ai dati tramite computer avverrà tramite un nome utente e una password associata attribuito al soggetto che effettua l'accesso;
- la password utilizzata deve essere di robustezza adeguata e contenere lettere maiuscole e minuscole, numeri e caratteri speciali. Non deve contenere elementi facilmente riconducibili all'utente;
- il nome utente e la password sono personali e non saranno condivisi con altri soggetti (a meno che non sia espressamente previsto);
- non dovranno essere inseriti dati personali in sistemi informativi non protetti da nome utente e password associata o protetti dal solo nome utente o dalla sola password;
- la password dovrà essere cambiata periodicamente con una diversa;
- nel caso di cessazione del rapporto di lavoro il dirigente dell'Ufficio dovrà chiedere la disattivazione dell'account presso qualunque sistema informativo utilizzato o server di rete;
- è vietato accedere ad un computer, alla rete o ad un sistema informativo utilizzando credenziali di altre persone;
- i documenti informatici contenenti dati personali non dovranno essere lasciati in cartelle di libero accesso o che consentono l'accesso a soggetti non autorizzati;
- non sia consentito a persone non autorizzate per iscritto dal Titolare o dal Responsabile di

utilizzare gli strumenti informatici, personal computers o video terminali, installati negli uffici;

- alla fine della sessione di lavoro i computer, eccetto quelli in funzione "H24", saranno spenti fisicamente;
- non si dovrà accedere a servizi online non consentiti;
- nei computer nei quali vengono utilizzati dati personali, ciascun dipendente porrà particolare attenzione ai programmi e ai servizi online utilizzati, al fine di escludere con ragionevole certezza la diffusione, anche involontaria, di dati personali ai quali ha avuto accesso in ragione delle autorizzazioni;
- non dovrà essere installato ed eseguito alcun software senza previa verifica dello stesso da parte del referente informatico del Dipartimento, a meno che il software non sia inserito in una lista dei software di uso consentito;
- non si dovrà tentare di acquisire privilegi di amministratore di sistema informatico;
- non si dovranno detenere chiavi di armadi o archivi ai quali non sia stato consentito l'accesso;
- non si dovrà collegare modem o altro dispositivo che consenta un accesso non controllato alla rete informatica regionale;
- il dipendente utilizza strumenti informatici con consapevolezza che sono di proprietà della Regione siciliana e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ogni dipendente è responsabile dell'utilizzo degli strumenti informatici che gli sono stati assegnati. Ogni utilizzo non inerente l'attività lavorativa è vietato in quanto può determinare disservizi o minacce alla sicurezza dei dati;
- saranno effettuate con procedure automatizzate copie di sicurezza (backup) settimanale del lavoro svolto nell'arco della settimana su un supporto che dovrà essere custodito separatamente dal computer ovvero su una cartella di un computer diverso, purché questa sia protetta da password personale che abiliti l'accesso esclusivo ai dati contenuti; nel caso di memorizzazione in servizi di cloud (ad es. Dropbox, google Drive, One Drive, WeTransfer ecc.) i documenti, ed in particolare quelli contenenti dati sensibili, dovranno essere criptati in maniera adeguata;
- le copie di backup potranno essere utilizzate esclusivamente per il fine per cui sono state effettuate, evitando di utilizzarle per accedere ai dati ivi contenuti tramite computer non autorizzati dall'Amministrazione;
- la consultazione della posta elettronica deve sempre essere improntata alla massima prudenza, non aprendo allegati ai messaggi di posta non richiesti o provenienti da soggetti sconosciuti o con elementi che tradiscano comportamenti dubbi;
- la navigazione su internet è consentita solo sui siti connessi alla attività lavorativa svolta, facendo attenzione a non condividere dati personali propri o altrui ed evitando di collegarsi a siti tramite link non richiesti;
- è vietato compiere azioni che potrebbero mettere a rischio i dati personali o creare falle nella sicurezza della rete o del computer utilizzato ad esempio scaricando file, programmi, audio o video non connessi all'attività lavorativa e di provenienza dubbia o non verificata.

I soggetti autorizzati al trattamento dei dati sono tenuti a collaborare, nell'ambito delle rispettive competenze, con il Titolare, il Responsabile, il sub-Responsabile e il Referente privacy, fornendo loro e fornire il supporto e l'assistenza necessaria allo svolgimento dei loro compiti nel rispetto del Regolamento UE 2016/679, del Dlgs 101/2018 e delle ulteriori disposizioni vigenti in materia.