AZIENDA SANITARIA PROVINCIALE

Istruzioni operative ai DIPENDENTI e COLLABORATORI
in materia di privacy

(Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D.Lgs. 196/2003)

A tutti i Dipendenti (neoassunti o già in servizio)
dell'A.S.P. di Ragusa

A tutti i Collaboratori (nuovi o già presenti)
nell'ambito dell'A.S.P. di Ragusa

In ottemperanza alle disposizioni del Regolamento Europeo per la protezione dei dati personali (GDPR 679/2016) e al Decreto Legislativo 196/2003 e successive modificazioni ed integrazioni (da ultimo D.lgs. 101/2018), tutti i dipendenti e i collaboratori di questa A.S.P. sono individuati come **"Autorizzati al trattamento dei dati personali"** e, nello svolgimento delle operazioni di trattamento dei dati, hanno l'obbligo di attenersi con scrupolo e diligenza alle seguenti istruzioni e ad ogni ulteriore indicazione, che potrà essere fornita dal ***Titolare del trattamento***(Direttore Generale) o da un Suo ***Delegato alla gestione delle attività di trattamento dei dati.***

N.B.: presso questa azienda, i *"Delegati"* sono tutti i Direttori di unità operativa complessa (**UOC**) e di unità operativa semplice e/o dipartimentale (**UOS UOSD**) nonché – per quanto riguarda le sole strutture "in staff" alla Direzione Aziendale – i Responsabili delle medesime strutture "di staff" (uffici o unità).

Trattamento di dati personali

L'art. 4 del GDPR 679/2016 definisce il trattamento di dati personali come *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e 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 dev'essere:

- effettuato secondo modalità tali da garantire la riservatezza;
- effettuato in modo lecito, corretto e trasparente nei confronti dell'interessato;
- effettuato per scopi determinati, espliciti e legittimi;
- rispettoso dei principi di necessità, pertinenza e non eccedenza rispetto alle finalità per le quali il dato è raccolto;

- idoneo a garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale
- effettuato per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono raccolti o successivamente trattati.

Obblighi formali

Ogni persona autorizzata al trattamento dati è tenuta a:

- attuare le misure necessarie per un corretto, lecito, sicuro trattamento, attenendosi alle istruzioni operative ed alle prescrizioni definite nella regolamentazione aziendale;
- utilizzare le banche dati informatiche esclusivamente attraverso le proprie credenziali di autenticazione da tenere riservate, e richiedere l'autorizzazione al proprio *Delegato Privacy* (Direttore UOC o UOS UOSD) per le modifiche e/o integrazioni del profilo autorizzativo che si rendessero necessarie;
- ottemperare agli obblighi di informazione e acquisizione del consenso, quando necessario e quando non altrimenti eseguito dalla propria struttura nei confronti degli interessati;
- controllare e custodire, durante il compimento dell'intero trattamento e fino alla consegna, gli atti e i documenti contenenti dati, personali sensibili o giudiziari, in modo da impedirne l'accesso a persone non autorizzate;
- informare il proprio *Delegato Privacy* in merito ad eventuali richieste dell'interessato volte a far valere i propri diritti in materia di privacy o di accesso;

Utilizzo e trasmissione dei dati

I dati oggetto di trattamento non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

Nessun dato personale può essere utilizzato o trasmesso all'esterno dell'Azienda, senza previa autorizzazione del Delegato alla gestione delle attività di trattamento dei dati o del Titolare.

Documenti cartacei

I dati presenti su documenti cartacei devono essere protetti mediante conservazione e gestione degli stessi in modo da evitarne la visibilità, la sottrazione, la riproduzione, l'alterazione o la distruzione abusiva.

- documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (*es. armadi o cassetti chiusi a chiave, uffici chiusi a chiave*).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie stampanti, fotocopiatrici o tavoli di lavoro.
- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative
- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili;
- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli autorizzati, i quali devono impedire l'accesso a persone prive di autorizzazione;
- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

Strumenti informatici

Al fine di garantire un corretto trattamento dei dati personali nel rispetto delle vigenti norme di legge, nonché delle misure di sicurezza che l'Azienda ha ritenuto idoneo adottare, è opportuno impiegare gli strumenti informatici con diligenza ed attenzione.

- Tutti i computer, incluso altro hardware, nonché i dati e il software nello steso contenuti (di seguito "PC") sono di proprietà dell'A.S.P. di Ragusa e sono forniti allo scopo di svolgere le mansioni affidate.
- Ogni informazione contenuta o memorizzata in qualsiasi PC cui si abbia accesso, di diversa natura e correlata all'attività dell'A.S.P., non può essere riprodotta o divulgata senza apposite autorizzazioni.
- Non si può usare, installare o copiare nel PC affidato dall'A.S.P. alcun software che non sia stato fornito dall'ente stesso e il cui uso non sia stato da questo autorizzato.
- Occorre evitare l'accesso al PC da parte di terzi non autorizzati e mantenere la natura riservata delle informazioni confidenziali
- La digitazione della password deve avvenire in modo discreto. Anche se i programmi non ripetono in chiaro la password sullo schermo, questa potrebbe essere letta guardando i tasti che vengono digitati. La password va mantenuta riservata e non va divulgata a terzi; non va consentito per esempio ad un collega di utilizzarla al proprio posto; non va trascritta su supporti (es. fogli, post-it) facilmente accessibili a terzi; non va lasciata memorizzata sul proprio PC.
- Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro ad intervalli fissi, tuttavia è buona prassi prendere l'abitudine di salvare direttamente i documenti in fase di elaborazione in modo da gestire personalmente i dati e non fare esclusivo affidamento sul sistema
- Per i dispositivi elettronici (cd-rom, pen drive etc.) si applicano gli stessi criteri dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento può passare facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni no sensibili, riponeteli sotto chiave non appena avrete finito di usarli. Non possono essere utilizzate pen drive per il trasferimento di dati particolari/sensibili a meno che non vengano protetti con sistemi di crittografia

Codice di comportamento dei dipendenti e dei collaboratori

Al fine di garantire un corretto trattamento dei dati personali nel rispetto delle vigenti norme di legge nonché delle misure di sicurezza che l'Azienda ha ritenuto idoneo adottare, è altresì opportuno rispettare i precetti di cui al "Codice Etico e di comportamento dell'Azienda Sanitaria Provinciale di Ragusa", tempo per tempo vigente, consultabile nel sito web aziendale Amministrazione Trasparente – Sezione Altri contenuti – Prevenzione della Corruzione

Massimario di scarto dei documenti

Al fine di garantire un corretto trattamento dei dati personali anche nel rispetto del principio generale (citato in premessa) secondo il quale il trattamento dei dati deve essere effettuato *"perun periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono raccolti o successivamente trattati"*, è altresì opportuno consultare, al bisogno, il *Piano di conservazione della documentazione aziendale (cd. massimario di scarto) a tutela del patrimonio documentale*

Per " Massimario" aziendale di conservazione e scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette

di gestire in modo organizzato l'archivio aziendale, conservando solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Il Data Protection Officer.
Dott.ssa Giovanna Di Stefano