Compiti e istruzioni ai designati in qualità di Responsabili "interni" del trattamento dei dati nell'ambito dell'organizzazione dell'Azienda Ospedaliera Ospedali Riuniti Marche Nord

PRINCIPI GENERALI

Ai sensi dell'art. 5 del Regolamento Europeo 2016/679 (GDPR) che prescrive i "*principi applicabili al trattamento dei dati personali*", il designato in qualità di Responsabile "interno" del trattamento è tenuto a garantire che ciascuna attività di trattamento dati effettuata nell'ambito della struttura di afferenza avvenga in osservanza dei seguenti principi di ordine generale:

- **liceità**, vale a dire nel rispetto delle Leggi, comprese quelle che regolano specifici settori;
- **correttezza**, vale a dire nel rispetto delle reciproche esigenze dell'Azienda e dell'Interessato, oltre agli obblighi derivanti dal quadro normativo;
- **trasparenza**, nel senso di assicurare la piena consapevolezza dell'Interessato, con particolare riferimento all'obbligo di rendere conoscibili all'utenza le modalità con cui i dati sono raccolti, utilizzati e consultati attraverso informazioni e comunicazioni facilmente accessibili, utilizzando un linguaggio semplice e chiaro.

I dati devono essere raccolti solo per **scopi**:

- **determinati,** vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, ossia, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;
- **compatibili** con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione degli stessi.

I dati devono, inoltre, essere:

- **esatti**, ossia, precisi e rispondenti al vero e, se necessario, **aggiornati**;
- **pertinenti**, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;

- **non eccedenti** in senso quantitativo rispetto allo scopo perseguito; ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine ed in mancanza dei quali non sia possibile il perseguimento del fine stesso;

- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle specifiche disposizioni di Legge cui è tenuto il Titolare. Al riguardo, il Titolare fa riferimento ai tempi stabiliti nel Prontuario aziendale disciplinante la conservazione della documentazione, nonché al Prontuario della Soprintendenza Archivistica della Regione Marche. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione non è più consentita. In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale devono** essere accuratamente conservati;

- **sicuri,** cioè deve essere garantita la sicurezza nel trattamento, compresa la protezione mediante misure tecniche e organizzative adeguate, atte a impedirne la perdita, distruzione o danno accidentale (integrità e riservatezza).

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dai principi fondamentali di **integrità, riservatezza** e **rispetto della dignità della persona fisica dell'interessato**, ovvero deve essere effettuato eliminando ogni rischio di impropria conoscibilità dei dati da parte di terzi e di perdita o distruzione del dato.

COMPITI SPECIFICI DEL RESPONSABILE

Il designato in qualità di Responsabile "interno" del trattamento, nell'ambito delle attività della propria Struttura che comportino operazioni di trattamento di dati personali, è tenuto a:

☐ trattare i dati personali osservando le vigenti disposizioni normative in materia di Privacy;

☐ verificare che ogni Incaricato, nello svolgimento delle operazioni strettamente connesse all'adempimento delle proprie funzioni, si attenga scrupolosamente alle istruzioni impartite curando, in particolare, il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati medesimi;

☐ adottare tutte le preventive misure di sicurezza ritenute idonee al fine di ridurre al minimo i rischi di distruzione, perdita e danno accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

☐ vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari;

☐ attenersi alle procedure aziendali relative alla gestione delle credenziali di autenticazione informatica per:
- l'attivazione di nuove profilazioni a fronte di nuove assunzioni o cambi mansione;
- la disattivazione delle credenziali di autenticazione informatica assegnate all'Incaricato per l'accesso ai singoli sistemi applicativi anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali (ad esempio cambio mansioni o trasferimenti ad altra UO);

☐ adottare idonee misure finalizzate a garantire la dignità delle persone e la riservatezza dei dati trattati in relazione a richieste o fruizioni di prestazioni sanitarie, secondo le indicazioni e i processi aziendali anche di natura informatica;

☐ proporre al Titolare del trattamento – in caso di stipula di contratti pubblici finalizzati all'acquisizione di beni e servizi che implichino attività di trattamento dati - la nomina dei soggetti esterni all'Azienda in qualità di Responsabili del trattamento ai sensi dell'articolo 28 del GDPR;

☐ garantire al Titolare la piena collaborazione in sede di effettuazione delle verifiche periodiche aventi ad oggetto l'accertamento del rispetto delle istruzioni impartite, anche per quanto attiene il rispetto delle misure di sicurezza;

☐ utilizzare il PC, internet e la posta elettronica attenendosi alle indicazioni e prescrizioni fornite dalla UOC Servizio Informatico;

☐ collaborare con il Responsabile per la transizione al digitale - nell'ambito dell'attuazione del piano triennale Agid - alla costante revisione dei processi verso la digitalizzazione;

☐ collaborare con il Responsabile della Protezione dei Dati ai fini dell'implementazione e costante aggiornamento del Registro delle attività di trattamento;

☐ effettuare, limitatamente all'ambito e agli aspetti di competenza, l'analisi dei rischi che incombono nei trattamenti di dati effettuati presso la Struttura di afferenza;

☐ informare il Titolare e il Responsabile della Protezione dei Dati in merito ad ogni questione avente particolare rilevanza in termini di impatto sulla protezione dei dati;

☐ consultare preventivamente il Titolare e il Responsabile della Protezione dei Dati nell'eventualità di trasferimento di dati personali in Paesi non appartenenti all'Unione Europea.