ISTRUZIONI OPERATIVE PER I PREPOSTI PRIVACY

I Preposti privacy in relazione alle attività di competenza della propria struttura o comunque correlate all'incarico attribuito, devono porre in essere tutte le azioni organizzative e gestionali necessarie a garantire che i trattamenti di dati personali effettuati avvengano nel rispetto delle disposizioni normative vigenti in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza, e delle disposizioni aziendali.

PRINCIPI GENERALI

I Preposti privacy devono:

- ✓ Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza. In attuazione del: principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto; principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità; principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
- ✓ Utilizzare le informazioni e i dati personali, in particolare i dati c.d. dati particolari, con la massima riservatezza, sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
- ✓ Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Preposto privacy di afferenza, garantendone la massima protezione in ogni attività di trattamento.
- ✓ Segnalare al Preposto privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- ✓ Astenersi dal comunicare a terzi e/o dal diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
- ✓ Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o da suo delegato.
- ✓ Collaborare alla implementazione e aggiornamento del Registro delle attività di trattamento del Titolare, con le modalità definite dal Comitato Data Protection e secondo le istruzioni ricevute, anche mediante utilizzo di apposito applicativo;
- ✓ coinvolgere tempestivamente e adeguatamente, in tutte le questioni riguardanti la protezione dei dati personali, il Responsabile della protezione dei dati (RPD) e collaborare con il medesimo per ogni questione relativa al trattamento dei dati personali, consentendo lo svolgimento di verifiche e audit presso la propria struttura;
- ✓ raccordarsi tempestivamente con il Titolare e con l'RPD nei casi di violazione di sicurezza che comporta violazione dei dati;

- ✓ assicurare che la comunicazione a terzi delle categorie particolari di dati personali, e dei dati relativi alle condanne penali e reati avvengano solo se previste da norma di legge o di regolamento;
- ✓ Non porre in essere trattamenti di dati personali diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;

OPERAZIONI SPECIFICHE

Trattamento dati degli interessati

- ✓ Verificare periodicamente che il trattamento e le sue modalità di esecuzione siano coerenti con le funzioni istituzionali dell'Azienda, con le attività di competenza della struttura o incarico assegnato e con la specifica attività in connessione della quale il trattamento viene effettuato;
- ✓ verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità determinate per cui sono stati raccolti e per le ulteriori finalità con esse compatibili; verificare periodicamente che le modalità del trattamento garantiscano comunque il diritto alla riservatezza dei soggetti terzi;
- ✓ verificare che il trattamento sia conforme alle disposizioni del GDPR e valutarne la temporanea sospensione, fino all'avvenuta regolarizzazione;
- ✓ assicurarsi che il trattamento delle categorie particolari di dati di cui all'art. 9 del GDPR e dei dati relativi a condanne penali e reati di cui all'art. 10 del GDPR nell'ambito di prestazioni di carattere amministrativo-gestionale, avvenga solo in relazione ai tipi di dati e di operazioni identificati con il Regolamento Regionale D.P.G.R. 12.02.2013 n. 6/R "Regolamento regionale per il trattamento di dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie Regionali, degli Enti vigilati dalla Regione", o in relazione a nuova regolamentazione regionale sopravvenuta.
- ✓ garantire la preventiva acquisizione del consenso nei casi in cui la normativa lo preveda;
- ✓ garantire la presenza, nei locali/aree aziendali di attesa o nelle quali si svolgono le attività di competenza della struttura di appositi cartelli/avvisi contenenti le informazioni generali sul trattamento dei dati agevolmente visibili al pubblico, fermo restando che queste devono eventualmente essere integrate da altre informative nel caso di trattamenti effettuati con modalità o per finalità o in ambiti particolari non dettagliati nelle informazioni generali;

Utilizzo strumenti aziendali

- ✓ Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- ✓ mail e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenenti dati riferiti alla salute;

- ✓ uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii;
- ✓ protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerà porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (es. un armadio o un cassetto chiusi a chiave, una cassaforte, etc.);
- ✓ assicurarsi che le apparecchiature elettroniche utilizzate, ivi comprese le attrezzature sanitarie, siano acquisite, inventariate, sottoposte a manutenzione e smaltite secondo quanto previsto dalle vigenti procedure aziendali.

Per il Regolamento aziendale per l'utilizzo delle risorse informatiche dell'Azienda Meyer si rinvia all'apposito allegato approvato con Delibera dalla Direzione Generale.

Individuazione dell'incaricato

È compito del Preposto privacy:

- ✓ individuare (anche per categorie) gli incaricati, cioè i soggetti afferenti alla propria struttura o assegnati alle attività di competenza autorizzati a trattare dati personali, mediante l'apposito modello predisposto dall' Azienda, consegnando l'originale della nomina all' interessato e conservandone una copia agli atti;
- ✓ autorizzare altresì al trattamento dei dati, in qualità di incaricati, mediante il medesimo modello di cui al punto precedente, soggetti non titolari di un rapporto di lavoro dipendente (soggetti con incarico libero professionale o in convenzione, borsisti, personale in formazione etc), presenti (anche occasionalmente) presso la struttura e che effettuino operazioni di trattamento dei dati personali nell'ambito delle attività di competenza, consegnando l'originale della nomina all'interessato e conservandone una copia agli atti;
- ✓ aggiornare l'individuazione degli incaricati in coerenza con cambiamenti organizzativi della struttura;
- ✓ ove necessario, specificare ed integrare le istruzioni impartite dal Titolare in relazione alle attività di propria competenza;
- ✓ verificare l'effettiva applicazione delle istruzioni impartite agli incaricati, in particolare sotto il profilo delle misure di sicurezza;
- ✓ assegnare i profili di accesso ai dati agli incaricati, in particolare, per i trattamenti di dati effettuati mediante procedura informatizzata, individuare idonei profili di autorizzazione, nel rispetto dei principi di necessità, pertinenza e non eccedenza informando immediatamente l'amministratore di sistema ai fini della disattivazione delle credenziali al venir meno delle condizioni organizzative che giustificano l'accesso dell'incaricato all'applicativo/banca dati;

- ✓ per le funzioni di Amministratore di sistema afferenti alle attività di competenza della struttura, individuare tra i propri incaricati gli Amministratori di sistema designandoli formalmente con atto scritto, previa valutazione deli' esperienza, capacità e affidabilità del soggetto designato;

Gestione delle misure di sicurezza organizzative e tecniche

È compito del Preposto Privacy:

- ✓ implementare e verificare l'effettiva attivazione delle misure (tecniche, informatiche, logiche, organizzative, logistiche e procedurali) che garantiscano adeguati livelli di protezione tali da ridurre al minimo o rimuovere i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- ✓ impedire il trattamento di dati da parte di soggetti non legittimati a qualsivoglia titolo, operanti nel proprio ambito di competenza; assicurarsi che nello svolgimento delle attività mediante strumenti elettronici ogni incaricato disponga di credenziali di accesso personali e riservate, e impartire adeguate istruzioni sulla scelta e sulla gestione della password;
- ✓ predisporre soluzioni organizzati ve/protocolli operativi interni che prevedano forme di vigilanza e/o di sicurezza rispetto all'accesso ai locali della propria struttura, di archivio e non, da parte di soggetti non autorizzati;
- ✓ coadiuvare il DPO nella verifica preventiva circa l'obbligatorietà dell'esecuzione della Valutazione di Impatto sulla Protezione dei dati -VIP;
- ✓ comunicare al Responsabile della protezione dei dati ogni notizia rilevante ai fini della protezione dei dati personali e della tutela della riservatezza;
- ✓ collaborare con il Responsabile della protezione dei dati personali provvedendo a fornire ogni informazione da questi richiesta; formulare adeguate proposte e richieste al Titolare, in particolare quando le soluzioni individuate non possano essere adottate facendo ricorso a mere misure o soluzioni organizzati ve interne;
- ✓ in caso di esternalizzazione/affidamento a terzi di attività/funzioni/servizi, procedere alla nomina del terzo a Responsabile del trattamento, mediante sottoscrizione dell'apposito format aziendale,
- ✓ mantenere costantemente aggiornato l’elenco dei Responsabili di cui ha perfezionato la nomina.

RESPONSABILITA'

Il Preposto privacy risponde al Titolare per l'inosservanza delle presenti istruzioni nonché per la violazione o inadempimento di quanto previsto dalla normativa in materia di protezione dei dati personali (fatte salve ulteriori fattispecie di responsabilità penale, a titolo personale, nonché amministrativa e contabile in sede di rivalsa).
Il ruolo di Preposto al trattamento dei dati non è suscettibile di delega. In caso di assenza o impedimento, le relative attribuzioni competono a chi lo sostituisce nell'attività istituzionale. La preposizione al trattamento è connessa all' incarico conferito, per cui viene automaticamente meno alla scadenza o alla revoca dell'incarico cui è correlata.