POLICY PRIVACY AZIENDALE

SCOPO

Lo scopo del presente documento è quello di descrivere i principi e gli obiettivi generali relativi al Sistema di Gestione Aziendale Privacy adottato dalla **ASL di Biella**, in qualità di Titolare, per la protezione delle persone fisiche/interessati con riguardo al trattamento dei dati personali e alla libera circolazione degli stessi.

NORMATIVA di RIFERIMENTO

La politica risponde:

- alle norme del Regolamento generale europeo per la protezione dei dati personali RGPD (o anche GDPR) n. 679/2016;
- alle disposizioni del D.lgs. n. 196/2003 recante il "Codice in materia di protezione dei dati personali"(c.d. Codice *privacy*), come novellato dal D.lgs. n. 101/2018 di armonizzazione della normativa nazionale italiana al Regolamento (UE);
- alle pronunce dell'Autorità Garante per la protezione dei dati personali;
- alle Linee guida del Gruppo di lavoro art.29;
- al sistema di gestione privacy implementato internamente all'azienda con riguardo, alle procedure, alla documentazione e alla modulistica di registrazione sviluppate.

AMBITO di APPLICAZIONE

La presente politica si applica all'Organizzazione del Titolare - **ASL di Biella** e in particolare:

- In linea con l'articolo 3 del Reg. (UE) n. 679/2016, la politica trova applicazione relativamente al trattamento dei dati personali, realizzato nell'ambito delle attività dell'organizzazione aziendale nel suo complesso, da parte del Titolare del trattamento e/o di tutti i soggetti che operino un trattamento dei dati personali all'interno della Azienda o per conto della stessa. Il documento si rivolge, in particolare, ai soggetti designati e a tutte le persone autorizzate al trattamento dei dati personali (compresi gli studenti e i tirocinanti) e ai soggetti esterni all'azienda (compresi i volontari) quando, in qualità di Responsabili del trattamento, trattano dati per conto del Titolare.

- In ottemperanza all'articolo 2 del Reg. (UE) n. 679/2016, la politica si rivolge al trattamento dei dati personali effettuato mediante l'ausilio di strumenti automatizzati o parzialmente automatizzati ed al trattamento non automatizzato dei dati personali, contenuti in archivio.

Per la corretta applicazione ed attuazione della presente politica e nell'ottica del miglioramento continuo della privacy, il Titolare ha definito un sistema organizzativo aziendale che si basa sull'implementazione di un **Sistema Gestione Privacy** conforme alla Normativa nazionale ed europea in materia di protezione dei dati personali, basato sulla gestione del rischio insito nel trattamento dei dati.
Il SGP applicato, favorendo la protezione dei dati e delle informazioni ed il coinvolgimento di tutti gli Operatori, permette il perseguimento sistematico, il monitoraggio continuo, la vigilanza sul funzionamento e la valutazione delle misure di sicurezza utilizzate e adeguate al rischio.

Il Titolare del trattamento/ ASL di Biella ha definito la presente Politica per la Protezione dei dati ed ha individuato nel contempo i mezzi e le risorse necessarie perché la politica sia compresa, attuata e mantenuta e si adopera affinché la stessa sia:

- **appropriata alle finalità e al contesto** dell'organizzazione e supporti gli indirizzi strategici;
- costituisca un **quadro di riferimento** per fissare gli obiettivi di sicurezza delle informazioni e protezione dei dati personali;
- comprenda l'**impegno** teso a soddisfare i requisiti applicabili e attinenti la sicurezza dei dati e delle informazioni e l'impegno per il miglioramento continuo del Sistema di Gestione Privacy;

OBIETTIVI e PRINCIPI

Atteso che per **dato personale** si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); e atteso che si considera* ***identificabile la persona fisica*** *che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*";

La **politica per la protezione dei dati personali**:

a) rappresenta l'impegno dell'organizzazione dell'ASL di Biella nei confronti delle persone fisiche a garantire la protezione dei dati personali e l'adozione di misure di sicurezza tecnico organizzative adeguate nel raggiungimento dei seguenti obiettivi:
   - **Riservatezza** → i Dati Personali non devono essere resi disponibili o divulgati a soggetti, entità o persone non autorizzate;
   - **Integrità** → i Dati Personali non devono subire modifiche; deve essere garantita la completezza delle informazioni Personali;
   - **Disponibilità** → i Dati Personali devono risultare accessibili ed utilizzabili su richiesta di un'autorità autorizzata e/o di un soggetto interessato;

b) si indirizza verso i nuovi imperativi di:
   - ***privacy by design*** concetto secondo il quale per ogni trattamento aziendale di dati personali sia garantita la protezione dei medesimi fin dalla progettazione dello stesso, con la valutazione dei rischi e con l' identificazione delle conseguenti misure di sicurezza applicabili, idonee a contenere tali rischi;
   - ***privacy by default*** definizione secondo la quale il titolare del trattamento mette in atto misure di sicurezza su base predefinita (*default settings*).

Il documento si ispira ai seguenti principi del Regolamento UE 679/2016 e del sistema privacy che devono essere osservati da tutti i soggetti coinvolti:

1. **Garantire** che i dati:
   - siano trattati in modo lecito, corretto e trasparente nei confronti dell'interessato **(«liceità, correttezza e trasparenza»**);
   - siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che un ulteriore trattamento non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali, a fini di archiviazione nel pubblico interesse, di ricerca

scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali **(«limitazione della finalità»**);

- siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati **(«minimizzazione dei dati»);**

- siano esatti e, se necessario, aggiornati; devono essere adottate tutte le misure previste per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati **(«esattezza»);**

- siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE 2016/679 a tutela dei diritti e delle libertà dell'interessato **(«limitazione della conservazione»**);

- siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante le misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali **(«integrità e riservatezza»**);

2. **Garantire** l'accesso sicuro alle informazioni, in modo da prevenire trattamenti di dati non autorizzati;

3. **Promuovere** l'adozione di procedure volte al rispetto di adeguati livelli di sicurezza e di protezione;

4. **Formare** e istruire tutto il personale addetto al trattamento dei dati personali affinché lo stesso acquisisca la piena conoscenza delle informazioni personali gestite e la capacità di valutazione della loro criticità, allo scopo di attivare le adeguate misure di sicurezza predefinite;

5. **Gestire** i fornitori che trattano dati personali per conto del Titolare/ ASL di Biella, attraverso processi di selezione e controllo che garantiscano la conformità privacy;

6. **Prevenire** il verificarsi di eventi che possano configurarsi come violazioni dei dati personali quali: la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso accidentale o illegale;

7. **Garantire**, al verificarsi di un'eventuale violazione dei dati, che sia attivata la procedura di gestione aziendale di *data breach* **(notifica al Garante e all'interessato)**;

8. **Assicurare** che siano fornite all'interessato, in caso di raccolta di dati personali presso il medesimo o qualora i dati non siano ottenuti direttamente dall'interessato, informazioni che rivelino: I dati di contatto del titolare, del responsabile della Protezione dei dati (RPD/DPO), del responsabile del trattamento, le finalità di trattamento, gli eventuali destinatari, il periodo di

conservazione, il diritto di proporre reclamo all'autorità di controllo, l'esistenza del diritto di chiedere al titolare l'acceso ai propri dati, la rettifica, etc. (**informativa all'interessato**);

9. **Assicurare** l'esercizio dei diritti da parte dell'interessato che ne faccia richiesta in osservanza alla procedura gestionale implementata;

10. **Sensibilizzare** tutta l'organizzazione in ordine al ruolo e alle responsabilità assegnate e nel rispetto del principio di riservatezza e di tutela dei diritti e delle libertà della persona fisica/interessato (**promozione della formazione e partecipazione agli eventi organizzati**).

VALORI AZIENDALI

Il diritto alla privacy è riconosciuto come un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana. Considerata la natura dei dati personali trattati in ambito sanitario, suscettibili di maggiore tutela, la politica privacy e il sistema di gestione aziendale, si adattano, inoltre, ai seguenti ulteriori valori dell' Azienda e ne favoriscono il perseguimento:

- la centralità dell'utente/paziente, con la partecipazione al processo di cura;
- la garanzia del rispetto del principio costituzionale di uguaglianza;
- il rischio, la prevenzione e la sicurezza;
- l'innovazione, la digitalizzazione, l'efficienza gestionale;
- l'alta specializzazione e professionalità;
- l'osservanza del segreto professionale e del segreto d'ufficio;
- l'integrazione tra le diverse unità operative/organizzative, interne all'azienda;
- la multidisciplinarità tra i diversi professionisti, interni ed esterni all' azienda sanitaria;
- la promozione della legalità e la tutela dei diritti e delle libertà personali;
- l'attenzione alla dignità della persona e allo specifico percorso di cura.

Il Titolare del trattamento/ASL di Biella è responsabile, secondo il **principio di *accountability***, del Sistema di Gestione Privacy adottato in coerenza con l'evoluzione del contesto aziendale, delle finalità del trattamento, del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Il Titolare mette in atto le misure tecniche organizzative adeguate al rischio e valuta le azioni da intraprendere al verificarsi di eventuali eventi negativi. Il Titolare è supportato dal Responsabile della protezione dei dati (DPO), opportunamente designato, e adeguatamente coinvolto nelle questioni riguardanti la protezione dei dati personali. Il DPO, in ambito di privacy, fornisce consulenza al Titolare e può essere contattato dagli interessati, svolge attività di vigilanza, coopera con l'autorità di controllo, funge da punto di contatto per la medesima autorità. Il Titolare del trattamento nella persona del Direttore generale ha individuato un Dirigente in qualità di Referente aziendale della privacy nonché un **Gruppo di Lavoro Permanente** per l'attuazione della normativa privacy, rappresentativo dei diversi settori di attività e costituito da professionalità multidisciplinari che intervengono in maniera operativa nelle attività di trattamenti di dati personali e che rappresentano il riferimento aziendale per le specifiche problematiche applicative della Normativa sulla privacy.

Luogo e data di approvazione	ASL di Biella Titolare del trattamento
_____	_____