Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

Azienda Socio Sanitaria Territoriale Nord Milano

REGOLAMENTAZIONE AZIENDALE IN APPLICAZIONE DELLA NORMATIVA VIGENTE SULLA RISERVATEZZA DEI DATI PERSONALI

PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 E

DEL D.LGS. 30 giugno 2003, n. 196 AGGIORNATO AL D.LGS. 10 agosto 2018, n. 101

ALEG-REGA-002 rev 1

APPROVATO CON DELIBERAZIONE 894/2020

Data	Descrizione	Redatto	Verificato	Approvato
09/12/2020	**Aggiornamento al D.LGS. 101/2018**	Dott.ssa Francesca Fasano (DPO)	Dott.ssa Teresa Leggieri (RQA)	Dott. Giovanni Palazzo (DAA)

1. NORME SULLA PRIVACY

Il presente Disciplinare contiene disposizioni attuative del **Regolamento UE 2016/679 (nel testo, anche "GDPR" – General Data Protection Regulation - o "Regolamento") e D.Lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali")**, aggiornato al **D.Lgs. 10 agosto 2018, n. 101 ("Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)")**, con lo scopo di garantire, nell'ambito delle strutture e servizi dell'Azienda Socio Sanitaria Territoriale Nord Milano, che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la medesima. L'ASST Nord Milano si impegna ad adottare misure di sicurezza, anche preventive, idonee ad evitare situazioni di rischio e di conformità o di alterazione dei dati.

2. DATI PERSONALI

E' **dato personale** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); 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 (art. 4 del GDPR).

Particolarmente importanti sono:

- i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. – e i **dati che permettono l'identificazione indiretta**, come un numero identificativo (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa dell'automobile);

- i **dati rientranti in particolari categorie**: si tratta dei dati c.d. "*particolari" o "sensibili*", cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento, all'articolo 9, ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

- i **dati relativi a condanne penali e reati e a connesse misure di sicurezza**: si tratta dei dati c.d. *"giudiziari"*.

3. TRATTAMENTO DEI DATI PERSONALI

Con l'espressione "trattamento", si intende qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

4. TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare del trattamento è l'ASST Nord Milano, il cui rappresentante legale è il Direttore Generale.
Il Titolare, tramite i "Responsabili Privacy di Unità" (RPU) da lui designati ai sensi dell'art. 2- quaterdecies del vigente Codice Privacy, adotta le decisioni sugli scopi e sulle modalità del trattamento, osservando e garantendo la corretta applicazione dei requisiti della normativa vigente in materia di tutela e sicurezza dei dati personali.

5. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO)

Il Responsabile della protezione dei dati personali, meglio conosciuto come "DPO" (Data Protection Officer), è una figura indipendente, deputata a sorvegliare l'osservanza degli obblighi sulla protezione dei dati posti in capo al Titolare o al Responsabile del trattamento. Tale figura è nominata per iscritto tramite deliberazione del Direttore Generale, al quale funzionalmente afferisce, sulla scorta di quanto previsto dal Regolamento (UE) 2016/679 (artt. 37-39) e delle specifiche indicazioni fornite dal Garante per la protezione dei dati personali. I suoi riferimenti e dati di contatto devono essere notificati al Garante e resi pubblici. Collabora con tutti i Dirigenti aziendali ed in particolare con il Dirigente del Servizio Informativo Aziendale.

6. UFFICIO PRIVACY

L'Ufficio Privacy opera all'interno della UOS Affari Legali, in Staff alla Direzione Generale, e costituisce il supporto operativo del DPO, che ne segue la formazione e la crescita professionale.
E' chiamato a dare applicazione alla normativa in materia di Privacy ed ai molteplici adempimenti che ne conseguono.
Si occupa, sotto la guida del DPO, della tenuta del Registro del trattamento del Titolare e dei Responsabili, della nomina dei Responsabili Privacy di Unità (RPU) e della predisposizione di modelli per la nomina degli autorizzati, della redazione di Informative e modulistica, della predisposizione di analisi dei rischi e valutazioni d'impatto, della gestione delle violazioni, dei riscontri alle richieste di esercizio dei diritti privacy e di tutto quanto è previsto dalle norme sotto il profilo documentale e giuridico.
Segue la contrattualizzazione dei Responsabili esterni del trattamento, nonché il riscontro alle richieste, alle nomine e ai documenti che pervengono all'Azienda. Collabora attivamente:

- con le funzioni di SIA, Risk Management, Qualità, URP, Comunicazione e con tutte le strutture sanitarie, sociosanitarie, amministrative;
- con funzioni analoghe e DPO di altre Aziende sanitarie, nell'ottica dello sviluppo di una rete comune di competenze.

In Azienda è presente il **GRUPPO AZIENDALE DI LAVORO SULLA PRIVACY**, espressione di significative e varie professionalità aziendali, per un indispensabile confronto e uno scambio di conoscenze finalizzate all'individuazione, all'analisi e alla disciplina di tutti i principali ambiti di trattamento.
Il Gruppo aziendale di lavoro è un organismo professionale che il Titolare pone a sostegno permanente del Responsabile della Protezione dei dati personali ai sensi dell'art. 38 , c. 2 del Regolamento (UE) 2016/679.
Si riunisce con cadenza mensile, o anche più breve, in caso di necessità.

7. RESPONSABILE PRIVACY DI UNITA' (RPU)

I Responsabili Privacy di Unità sono nominati dal Direttore Generale e sono individuati nelle seguenti funzioni aziendali:

- Direttore UOC
- Dirigente USSD
- Dirigente UOS di staff.

L'atto di nomina viene notificato per iscritto ai soggetti individuati.
La designazione dei sostituti in caso di assenza o impedimento corrisponde a quanto previsto dagli atti deliberativi aziendali attuativi del CCNL 19.12.2019, art. 22 (per l'Area della Dirigenza Medica e Sanitaria) e del CCNL 8.6.2000, art. 18 (per l'Area della Dirigenza PTA).

I Responsabili Privacy di Unità compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza e in particolare hanno il dovere di:

- osservare gli obblighi riportati nell'Accordo di nomina;
- osservare e fare osservare le precauzioni individuate nei Documenti sul corretto trattamento dei dati personali elaborati dall'Azienda;
- osservare quanto disposto dall'art. 30 del Regolamento UE sulla tenuta del Registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, con le modalità concordate con l'Ufficio Privacy e nell'ambito delle indicazioni da questo ricevute.

8. TRATTAMENTI DI DATI AFFIDATI ALL'ESTERNO: CONTITOLARI E RESPONSABILI ESTERNI DEL TRATTAMENTO

Negli accordi con altre Strutture o Enti e nei contratti di affidamento di attività o di servizi all'esterno dell'Azienda, deve essere inserita un'apposita disciplina in cui il soggetto convenzionato o affidatario si impegna all'osservanza delle norme di legge sulla protezione dei dati personali e ad osservare quanto disposto da ASST Nord Milano in materia di trattamento di tali dati, in ordine ai trattamenti effettuati in forza del rapporto contrattuale. Detto Accordo è predisposto e conservato dalle Strutture che si occupano di Contratti e Convenzioni con la collaborazione, ove necessaria, dell'Ufficio Privacy. L'elenco degli Accordi viene inviato semestralmente all'Ufficio Privacy e al DPO.

La disciplina contrattuale sulla privacy dovrà quindi tenere conto degli obblighi derivanti da rapporti di contitolarità (art.26 del Regolamento UE) o dalla nomina a Responsabile del trattamento del fornitore (art.28 del Regolamento UE), che costituiscono le due tipologie di Accordo da stipulare con soggetti esterni.

9. AUTORIZZATI AL TRATTAMENTO

Ai sensi dell'art. 2-quaterdecies del vigente Codice Privacy (D.Lgs. 196/2003) e dell'art. 29 GDPR - l'Azienda autorizza al trattamento dei dati personali il personale dipendente che nell'ambito delle funzioni attribuite è tenuto ad effettuare delle operazioni (inclusa la sola custodia) sui data base cartacei ed informatici aziendali.

Per designare le figure autorizzate al trattamento, è stato predisposto un modello che viene sottoscritto anche dal Responsabile Privacy di Unità, sulla base dell'assetto organizzativo vigente e degli ambiti di trattamento dei dati personali consentiti. Nella comunicazione è chiaramente prevista la sottoscrizione di un'apposita clausola di riservatezza in relazione ai dati trattati.

E' prevista l'individuazione in qualità di "autorizzati" anche per le figure professionali che hanno instaurato formali rapporti con l'Azienda, pur in assenza di un vincolo di dipendenza: collaboratori, tirocinanti, volontari, specializzandi, docenti e figure assimilabili alle predette categorie.

I Responsabili Privacy di Unità attesteranno all'Ufficio Privacy l'avvenuta sottoscrizione dell'atto di nomina in qualità di autorizzato/i di tutti gli operatori, anche non dipendenti, assegnati o comunque presenti nelle loro Strutture.

10. CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato.
Oggetto del trattamento devono essere i soli dati essenziali per svolgere le attività istituzionali di competenza.
I dati personali devono essere trattati in modo lecito, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.
Ogni comportamento che si discosti da tali disposizioni è punibile a norma di legge, contratto, Regolamento.

I Responsabili Privacy di Unità e i Responsabili esterni del trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non necessari, non possono essere utilizzati. L'atto che li contiene seguirà le disposizioni in vigore in ordine ai termini di conservazione e di scarto legale.

Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo od ispettivo anche su richiesta di altri soggetti.
I trattamenti consentiti vengono elencati nel Registro del trattamento del Titolare e del Responsabile del

trattamento.
I trattamenti di dati effettuati utilizzando le banche dati di diversi Titolari sono utilizzati nelle sole ipotesi espressamente previste dalle norme.

11. INFORMATIVA ALL'INTERESSATO

Le informative vengono elaborate e distribuite formalmente dall'Ufficio Privacy, previa validazione della UOS Qualità e Risk Management, tenendo conto degli ambiti di trattamento stabiliti dal Registro e dalle regole di seguito descritte.

Il Responsabile Privacy di Unità verifica che gli autorizzati forniscano all'interessato, oralmente o per iscritto, antecedentemente o al momento della raccolta dei dati, l'informativa aggiornata di cui agli artt. 13-14 del Regolamento UE 2016/679.

L'informativa deve specificare:

- chi è il Titolare del Trattamento, fornendo opportuni dati di contatto;
- come contattare il Responsabile della protezione dei dati/DPO;
- quali sono le finalità del trattamento, ossia per quale scopo si intende raccogliere i dati personali dell'interessato;
- oltre alle finalità del trattamento il Titolare **DEVE SEMPRE** specificare la **base giuridica** del trattamento e la presenza e la tipologia di eventuali legittimi interessi;
- in relazione ai destinatari dei dati, **va precisato se l'organizzazione intende trasferire i dati personali in Paesi terzi** indicando, in caso affermativo, le garanzie previste e gli accordi che le prevedono;
- **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione;
- se la comunicazione dei dati personali è obbligatoria oppure facoltativa e le conseguenze della mancata comunicazione dei dati stessi;
- l'esistenza o meno di un processo decisionale automatizzato, con le eventuali conseguenze;
- tutti i i diritti dell'interessato.

Se i dati personali non sono acquisiti solo presso l'interessato, il Titolare dovrà riportare nell'informativa:

A. le categorie di dati personali in questione
B. la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'informativa deve avere forma **concisa, trasparente, intelligibile per l´interessato e deve essere facilmente** accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori prevedere informative idonee.

L´informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato cartaceo**, anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra. Il Regolamento ammette, soprattutto, l´utilizzo di **icone** per presentare i contenuti dell´informativa in forma sintetica, **ma solo "in combinazione" con l´informativa estesa**.

L´informativa deve essere esposta nei locali in cui si esegue la prestazione e fornita all´interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l´interessato – art. 13 del GDPR). Nel caso di dati personali non raccolti direttamente presso l´interessato (art. 14 del GDPR), l´informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all´interessato).

12. DIRITTI DELL'INTERESSATO

In base a quanto stabilito dal capo III del Regolamento europeo, l'interessato può esercitare i seguenti diritti in relazione ai propri dati personali:

1. ACCESSO
La persona i cui dati sono oggetto di trattamento ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati e quali ne siano le caratteristiche: cfr. nota 1.

2. RETTIFICA
L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

3. CANCELLAZIONE (OBLIO)
La persona i cui dati sono oggetto di trattamento ha diritto, a determinate condizioni, di ottenere dal Titolare del trattamento la cancellazione dei dati personali che la riguardano senza ingiustificato ritardo e di conseguenza il Titolare del trattamento, senza ingiustificato ritardo, ha l'obbligo di cancellare i dati stessi.

4. LIMITAZIONE
La «limitazione di trattamento» è il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento nell'immediato o in futuro. La limitazione consiste, a determinate condizioni, nell'impedire qualsiasi tipo di operazione sui dati contrassegnati ad esclusione della conservazione.

5. PORTABILITA'
La persona i cui dati sono oggetto di trattamento ha diritto, a determinate condizioni, di riceverli in un formato strutturato, di uso comune e leggibile da dispositivo automatico e ha diritto di trasmetterli ad un altro titolare se il trattamento si basava sul consenso oppure era effettuato con mezzi automatizzati.

6. OPPOSIZIONE
La persona i cui dati sono oggetto di trattamento ha diritto, a determinate condizioni, di opporsi allo stesso a meno che il Titolare del trattamento dimostri l'esistenza di motivi legittimi cogenti prevalenti.

L'interessato può esercitare i suoi diritti in materia di privacy in due diversi modi:

- DIRETTAMENTE: tramite Domanda orale o scritta ovvero attraverso apposito Modello di esercizio dei diritti (presente sul sito aziendale alla Sezione Privacy)
- TRAMITE UN DIFENSORE: previa apposita procura o delega che va allegata all'istanza.

L'Ufficio Relazioni con il Pubblico accoglie le richieste e interpreta i bisogni dell'interessato, guidandolo all'occorrenza nella compilazione del Modello per l'esercizio dei diritti, sopra citato.

Il Modello viene trasmesso all'Ufficio Privacy, che svolge funzioni di "Gestione reclami privacy", per la prevenzione del contenzioso sulla riservatezza dei dati personali.

La **richiesta deve essere formulata liberamente e senza costrizioni** e non deve essere già stata presentata

[1] in base all'art.15 del Regolamento, la persona interessata ha diritto di conoscere:
a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

con un intervallo di **tempo inferiore a 30 giorni**.
Il personale che riceve la richiesta deve avere **conferma dell'identità del richiedente**.
Per le richieste che pervengono via email, è necessario allegare la scansione di un proprio documento di riconoscimento.

La richiesta della persona interessata può essere soddisfatta anche qualora questa dovesse esercitare i propri diritti attraverso delega scritta a persona fisica, enti, associazioni od organismi, titolati ad agire per suo conto.
Il soggetto che agisce per conto della persona interessata esibisce o allega copia della delega sottoscritta dall'interessato e presentata unitamente a fotocopia non autenticata di un documento di riconoscimento dell'interessato medesimo.

E' possibile richiedere informazioni anche per conto di un defunto, solo se si dimostra che si ha un interesse personale o si opera nell'interesse del deceduto o per ragioni familiari meritevoli di protezione, come più dettagliatamente descritto al termine del presente capitolo.

Una volta raccolta la richiesta di esercizio dei diritti, l'Ufficio Privacy ne valuta il contenuto in collaborazione con il Responsabile del settore interessato e il DPO e formula una risposta scritta che, a seconda delle specifiche situazioni, accoglie totalmente o parzialmente la richiesta.

L'Ufficio Privacy dà riscontro all'interessato in **forma concisa, trasparente, intelligibile e facilmente accessibile**, con un linguaggio semplice e chiaro, attraverso tre possibili modalità:

1) **PER ISCRITTO**: il riscontro viene trasmesso mediante lettera raccomandata o (prioritariamente) attraverso la posta elettronica;
2) **ORALMENTE**, purché sia comprovata con altri mezzi l'identità dell'interessato. In questo caso l'incaricato ne prende sinteticamente nota in un registro;
3) con semplice **PRESA VISIONE** delle informazioni, anche attraverso strumenti elettronici, purché la comprensione sia agevole, tenuto conto della quantità e qualità delle informazioni.

L'Ufficio Privacy è tenuto a dare riscontro alla richiesta massimo entro **30 giorni dalla data di inoltro o entro ulteriori 30 giorni** nel caso in cui la risposta sia particolarmente complessa; in ogni caso, **entro il trentesimo** giorno deve essere data comunicazione scritta delle motivazioni del ritardo. Possono essere applicati termini più restrittivi a vantaggio dell'interessato.

L'Ufficio rilascia le informazioni richieste a titolo gratuito. Se le richieste dell'interessato sono manifestamente infondate o eccessive (ad esempio, ripetitive), l'operatore, su istruzione del proprio Responsabile, provvede a:

a) comunicare la necessità di far addebitare un contributo spese, tenendo conto dei costi vivi di riproduzione sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) può legittimamente rifiutarsi di soddisfare la richiesta.

In base a quanto stabilito dal vigente D.Lgs. 196/2003, i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al Titolare del trattamento, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attivita' di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attivita' svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalita' inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonche' alla tutela della loro stabilita';
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identita' del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

Ai sensi dell'art. 2-terdecies **(Diritti riguardanti le persone decedute)** del vigente D.Lgs. 196/2003, i diritti di cui agli artt. 15 - 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione.

L'esercizio dei diritti non e' ammesso nei casi previsti dalla legge o quando l'interessato lo ha espressamente vietato in vita, con dichiarazione scritta presentata al Titolare del trattamento o a quest'ultimo comunicata. La volonta' dell'interessato di vietare l'esercizio dei diritti deve risultare in modo non equivoco e deve essere stata specifica, libera e informata; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti. In ogni caso, il divieto non puo' produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.

13. REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

Il Registro delle attività di trattamento del Titolare (Registro), come definito dall'art. 30 del Regolamento Europeo 2016/679, costituisce il nucleo del sistema di protezione dei dati aziendali.
Insieme ad una oculata e puntuale allocazione dei ruoli e delle responsabilità, rappresenta il punto di partenza della strategia aziendale per la messa a punto di un'efficace Sistema aziendale di gestione della privacy.
Il Registro è composto da una serie di Schede, che corrispondono alle attività delegate ai Responsabili Privacy di Unità.
Lo scopo del Registro è infatti quello di censire le attività di trattamento effettuate dal Titolare e dai singoli RPU, individuando e mappando processi e relative responsabilità.
Come strumento di rilevazione (Scheda di Registro), viene usato il Modello presente nella pubblicazione: "Manuale RPD – Linee Guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea, Regolamento (UE) 2016/679", pubblicato sul sito dell'Autorità Garante per la Privacy.
Durante il percorso di definizione, censimento e mappatura delle attività di trattamento, sono stati individuati gli elementi fondamentali che le costituiscono (soggetti coinvolti, finalità, legittimazione legale, categorie di dati e di interessati, etc) e sono stati altresì censiti gli altri elementi richiesti, quali: ambito del processo, applicativi correlati e strumenti in dotazione.
Il Registro è tenuto in forma scritta, in formato elettronico; ne viene conservata una copia cartacea per una più immediata accessibilità.
Il costante e puntuale censimento delle attività che comportano il trattamento di dati personali è propedeutico alla valutazione dei profili di rischio e dell'analisi d'impatto sulla protezione dei dati, alla gestione degli eventuali incidenti di sicurezza, alla verifica della corretta allocazione delle responsabilità; ma la sua funzione è in primis quella di garantire il rispetto dei diritti degli interessati.
Si considerano integrativi del Registro:

- la copia dell'Organigramma aziendale delle Strutture Complesse, Semplici e Semplici Dipartimentali, tratto dall'ultimo Piano di Organizzazione Aziendale;
- l'elenco delle misure di sicurezza, tecniche e organizzative, applicate ad oggi in Azienda;
- l'elenco delle apparecchiature che prevedono trattamento dei dati personali, che integra quanto già eventualmente presente nelle Schede di Registro;
- l'Elenco dei Responsabili esterni del trattamento dei dati.

I Responsabili del trattamento attesteranno semestralmente all'Ufficio Privacy la variazione o meno delle attività elencate nel Registro.

14. ANALISI DEI RISCHI E VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

L'ASST Nord Milano mediante l'Ufficio Privacy, l'UOC SIA e i Responsabili Privacy di Unità predispone annualmente un Documento di Analisi dei rischi, e lo aggiorna tenendo conto delle criticità gestite e delle

azioni di miglioramento implementate.

Sui processi a rischio elevato il Responsabile del trattamento e il SIA collaborano con l'Ufficio Privacy nella stesura di opportuna valutazione d'impatto.
Come da normativa vigente e da Linee guida del Garante, si dovrà tenere conto, quando richiesto dalla tematica, dell'opinione di rappresentanti degli interessati al trattamento e del Responsabile della protezione dei dati personali/DPO.
L'organizzazione fornisce istruzioni ai suoi Responsabili del trattamento per valutare in modo approfondito i rischi specifici di ASST Nord Milano e compilare ai sensi di legge le valutazioni d'impatto.

I documenti di analisi generale dei rischi e valutazione d'impatto vengono sottoposti all'attenzione del Direttore Generale che, valutati i contenuti, provvede alla loro approvazione finale con atto deliberativo.

15. ADOZIONE MISURE DI SICUREZZA

E' responsabilità dell'Ufficio Privacy e del Dirigente del SIA, supportare:

- l'Azienda nella definzione di misure organizzative e tecniche generali, ossia misure che cautelino trasversalmente i data base sotto la titolarità dell'Azienda;
- i Responsabili Privacy di Unità nella definizione di misure organizzative e tecniche per la gestione dei rischi connessi alla propria area di competenza.

Ciascun Responsabile Privacy di Unità è tenuto ad applicare nella propria Struttura le misure di sicurezza organizzative e tecniche stabilite e vigilare sulla loro corretta adozione, anche prevedendo momenti di formazione destinati ai propri collaboratori, opportunamente documentati.

16. REVISIONE PERIODICA DEL DOCUMENTO

Tenendo conto che il quadro giuridico di riferimento è in costante evoluzione, l'ASST Nord Milano stabilisce che con il supporto del DPO verificherà annualmente il presente documento, ponendo in evidenza correzioni o integrazioni.

Il presente Regolamento, dopo l'adozione, sarà pubblicato sul Sito aziendale, sezione Privacy.