REGOLAMENTO AZIENDALE IN MATERIA DI PRIVACY

Aggiornamento 2022

Indice

ALLEGATI **Pag. 15**

Allegato 1 – Delegato al trattamento
Allegato 2 – autorizzazione dipendenti
Allegato 3 – autorizzazione studenti e volontari
Allegato 4 – nomina Amministratore di sistema
Allegato 5 – autorizzazione operatori centro antiviolenza
Allegato 6 – nomina Responsabile del trattamento (esterno)
Allegato 7 – nomina Responsabile del trattamento per professionisti

1. DEFINIZIONI PRINCIPALI

1.1 CATEGORIE DI DATI

1.1.1 "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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

1.1.2 "Dato particolare" – dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona.

1.1.3 "Dati relativi alla salute" – sono inclusi nella definizione di dato particolare (vedi punto 1.1.2) e sono definiti come i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

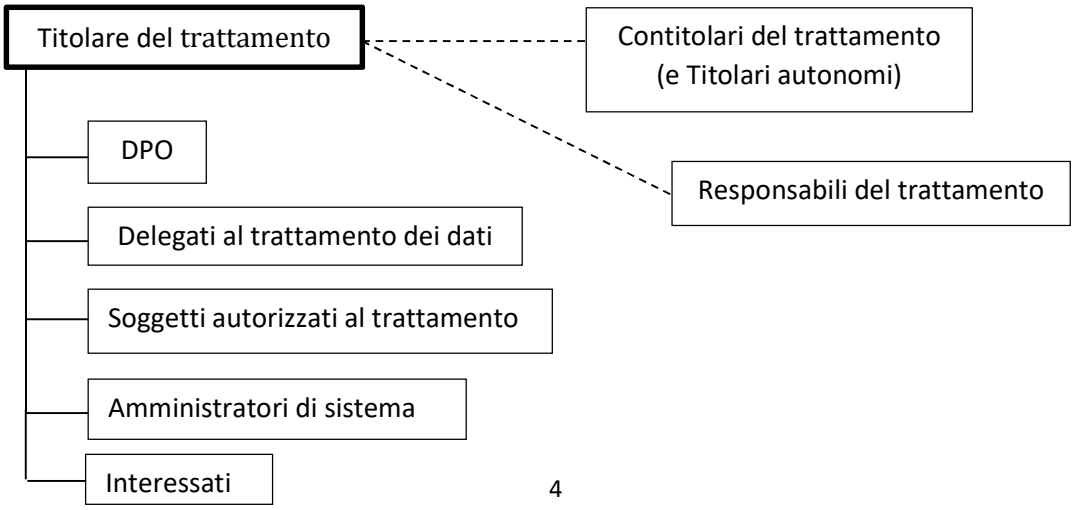
1.1.4 "Dati genetici" – dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

1.1.5 "Dati biometrici" – dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

1.1.6 "Dati giudiziari" – dati relativi alle condanne penali, ai reati o a connesse misure di sicurezza.

1.1.7 "Trattamento" – 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.
L'ASST Ovest Milanese nell'esercizio delle proprie funzioni garantisce che il trattamento dei dati avvenga nel rispetto dei principi di cui all'art. 5 del Reg. UE 2016/679 (liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza ecc.), e in modo conforme alle finalità rappresentate nelle informative.

2. RUOLI, FIGURE E ORGANISMI AZIENDALI



2.1 "Titolare del trattamento" – la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (Reg. UE 2016/679 art. 4).
Pertanto Titolare del trattamento di tutti i dati personali è l'ASST Ovest Milanese.

2.2 "Responsabile Protezione Dati" – RPD (Data Protection Officer – DPO) - In ASST Ovest Milanese il Responsabile della Protezione dei Dati, qualora interno all'organizzazione, è nominato con Delibera del Direttore Generale che, valutati i requisiti professionali, ne stabilisce la durata dell'incarico e i compiti, tenuto conto delle specificità organizzativa dell'azienda. I dati di contatto del DPO devono essere notificati secondo le procedure del Garante.
L'articolazione delle funzioni del DPO di cui sopra tiene conto di quanto stabilito agli artt. 37-38-39 del Reg. UE 2016/679, rispetto alla posizione e ai compiti ivi descritti.
Il DPO supporta le strutture interessate nella stesura e nell'aggiornamento dei modelli e della documentazione relativa all'ambito "privacy" nei processi aziendali, fornendo la propria consulenza al Gruppo di lavoro privacy e ai delegati.
Inoltre, svolge attività di supporto alla Direzione per valutare eventuali data breach, svolge attività di sensibilizzazione del personale promuovendo iniziative formative o veicolando contenuti informativi su provvedimenti, linee guida e particolari situazioni che hanno attinenza con le attività dell'ASST.
Il DPO propone al titolare le risposte alle richieste di esercizio dei diritti degli interessati nelle modalità di cui al punto 4.3 e supporta il titolare nella gestione dei reclami.
Il DPO svolge la propria attività di sorveglianza attraverso controlli a campione e/o audit.

2.3 Delegati al trattamento dei dati (ex Responsabili interno al trattamento) (**allegato 1**) come indicato all'art. 2-quaterdecies D.lgs 196/2003 modificato dal D.lgs 101/2018) – Tenuto conto della complessità e della eterogeneità organizzativa dell'ASST è opportuno che alcune funzioni del Titolare siano distribuite e delegate alle figure dirigenziali, di seguito indicate:

- i Direttori di Unità Operativa complessa (UOC) dell'area clinica, amministrativa e tecnica;
- i Responsabili di Unità Operativa Semplice Dipartimentale (UOSD) dell'area clinica, amministrativa e tecnica;
- i Responsabili di Unità Operativa Semplice di Staff (UOS di Staff);
- i Responsabili di specifiche funzioni assegnate agli staff della Direzione strategica (tranne il DPO che è soggetto autorizzato al trattamento);

La designazione di Delegato è legata al conferimento dell'incarico di responsabilità della struttura o funzione e comporta lo svolgimento di attività di supporto al Titolare, nel controllo, nella supervisione e nell'attuazione delle istruzioni e delle policy aziendali. Tale designazione è attribuita con l'atto di assunzione dell'incarico di una delle strutture/funzioni sopra indicate, in concomitanza della sottoscrizione del contratto di lavoro o del provvedimento di conferimento dell'incarico principale. Di ogni conferimento di delega, ne viene data comunicazione all'ufficio privacy (S.C Affari Generali e legali) per l'aggiornamento dell'elenco.
Il "Delegato" svolge tutte le funzioni previste all'**allegato 1** quale atto di delega delle funzioni del Titolare. La nomina di Delegato è conferita dal Titolare in funzione delle esigenze organizzative aziendali.
Inoltre i Delegati possono integrare le istruzioni già date dal Titolare con le specifiche riguardanti l'attività della struttura di riferimento in cui operano, come indicato nel modello di cui all'**allegato 1**.
Il Delegato, tra l'altro:

1. è parte nel procedimento di valutazione del data breach, secondo le modalità indicate nello specifico Regolamento aziendale di cui al punto 8.
2. Partecipa alla redazione e all'aggiornamento del Registro dei trattamenti, con la compilazione della scheda di informazione riguardanti le proprie attività, in collaborazione con il Titolare/DPO.
3. Il Delegato informa il Titolare e il DPO nel caso in cui si renda necessario un nuovo trattamento di dati, così da poter effettuare la Valutazione d'impatto (DPIA art. 35 del Reg.

UE 2016/679) prima di procedere al trattamento ed è parte del processo di valutazione d'impatto, secondo le modalità e il ruolo indicati nelle specifiche istruzioni aziendali

Il delegato sottoscrive l'autorizzazione al trattamento anche dei soggetti esterni all'organizzazione (studenti, tirocinanti, volontari ecc.) che accedono ai dati personali di cui l'ASST è Titolare (**allegato 3**).

2.4 "Soggetti autorizzati al trattamento" (art. 4 punto 10, art. 28 c.3 lett. b) e art. 29 del Reg. UE 2016/679) – sono le persone fisiche autorizzate e designate (art 2-quaterdicies D.Lgs 196/03) in forma scritta a compiere le operazioni di trattamento dal Titolare (o dal suo Delegato) e/o dal Responsabile. Pur non essendo prevista in modo specifico la figura dell' "incaricato", nel Regolamento UE 2016/679, si parla comunque di "persone autorizzate" al trattamento dei dati.
I soggetti autorizzati al trattamento dei dati all'interno dell'ASST Ovest Milanese sono tutti i dipendenti che quotidianamente gestiscono i dati, sia su supporto cartaceo che su supporto informatico (medici, infermieri, tecnici, ausiliari, amministrativi etc).
Sono altresì autorizzati al trattamento i soggetti (studenti, tirocinanti, volontari ecc.) che, pur essendo esterni ai ruoli aziendali, sono integrati nel contesto organizzativo per le attività loro affidate e accedono ai dati personali di cui l'Azienda è titolare. (vedi punto 2.10 e **allegato 3**)
I dipendenti ricevono un atto di autorizzazione al trattamento con le istruzioni necessarie (**allegato 2**) per lo svolgimento della propria attività: in tali istruzioni si concretizza la "diretta autorità" del Titolare, sui cui grava, pertanto, l'obbligo di vigilare l'operato degli autorizzati stessi. Il Delegato al trattamento, come indicato al punto 6 della nomina di delegato, può integrare le istruzioni del Titolare.

Al dipendente autorizzato al trattamento vengono rilasciate le credenziali di accesso ai sistemi in uso presso la struttura di appartenenza, su richiesta del Dirigente, Delegato al trattamento, il quale dovrà farsi carico anche della richiesta di revoca degli accessi in caso di spostamento del personale secondo quanto definito nel "regolamento aziendale per l'utilizzo dei sistemi informativi ai sensi dell'art. 32 del regolamento UE 2016/679". La richiesta va presentata alla S.C sistemi informativi aziendali.

2.5 "Interessati" – Sono le persone fisiche cui si riferiscono i dati personali oggetto di trattamento (pazienti, utenti, dipendenti fornitori ecc.)

2.6 "Amministratori di Sistema" - La figura dell'Amministratore di sistema è prevista nel provvedimento del Garante del 27 novembre 2008: "Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi**".**
In azienda sono amministratori di sistema: tecnici del SIA e tutti coloro che in azienda svolgono attività di programmazione, gestione e sviluppo di software, applicativi, incluse piattaforma web.
Il Responsabile della UOC SIA, in quanto Delegato al trattamento, individua e nomina gli Amministratori di sistema tra i soggetti che svolgono la loro attività all'interno del SIA in funzione delle aree di competenza.
Allo stesso modo i Responsabili di altre strutture (laboratori, DAPSS, Ingegneria clinica, controllo di gestione, ecc.), individuano se e quali tra i loro collaboratori devono svolgere attività di Amministratori di sistema al fine del conferimento della specifica nomina da parte del Delegato (vedi punto 7 della nomina di Delegato).

2.7 "Responsabili del Trattamento" – vengono definiti dal Reg. UE 2016/679 come le persone fisiche o giuridiche, le autorità pubbliche, i servizi o altri organismi che trattano dati personali per conto del titolare del trattamento (Reg UE 2017/679 art. 4 c.1 punto 8 e art. 28) nell'interesse dell'Azienda per finalità connesse all'esercizio delle funzioni istituzionali, sulla base di accordi giuridici.
Il ruolo e la funzione del Responsabile sono definite nello stesso art. 28 del Reg UE 2016/679.
La normativa prevede che tali soggetti debbano obbligatoriamente essere investiti di specifica responsabilità in materia in quanto per l'esecuzione di specifiche attività contrattualizzate trattano dati personali e categorie particolari di dati di titolarità di ASST Ovest Milanese. Sono quindi soggetti esterni specificatamente designati con un atto di nomina, il cui modello è predefinito in azienda, correlato all'accordo/contratto/convenzione principale.

Gli uffici che gestiscono i rapporti con soggetti nominati "Responsabili del trattamento" ne tengono un elenco aggiornato a disposizione del Responsabile della Protezione dei Dati e del Titolare.
Il Responsabile del trattamento può ricorrere ad un sub responsabile nelle modalità indicate dall'art. 28 c. 2 del Regolamento UE e disciplinate nel modello di nomina di Responsabile del Trattamento dei dati, in uso in azienda.
Il Delegato al trattamento dei dati di cui al punto 2.3, nell'esecuzione delle procedure di stipula di un contratto/convenzione/accordo, valuta l'esistenza delle condizioni per il conferimento della nomina di Responsabile del Trattamento (esterno) al soggetto controparte, utilizzando il modello allegato al presente documento (**allegato 6**). Tranne le ipotesi in cui la nomina di Responsabile è parte integrante di un bando, qualora si ravvisi la necessità di apportare deroghe al modello per dettagli di adeguamento alle esigenze rappresentate in merito allo specifico contratto, prima della sottoscrizione, queste sono valutate dal Delegato, che può sentire anche il parere del DPO. Tale procedura è necessaria affinché non venga modificata la sostanza delle policy che con il conferimento della nomina il Titolare del trattamento intende adottare nei confronti dei Responsabili.
La nomina di Responsabile del Trattamento, nelle procedure di acquisizione di servizi e forniture, viene conferita seguendo le seguenti modalità:

1) in caso di gara la nomina diventa parte del bando quale lex specialis;
2) in caso di adesione a bandi consip o altre gare aggregate, il Delegato invia la nomina di Responsabile del trattamento nella fase antecedente alla sottoscrizione del contratto quale parte integrante dello stesso;
3) in caso di affidamento diretto la nomina è contestuale alla sottoscrizione del contratto e ne diventa parte integrante.

- Compilazione del modello di nomina di Responsabile (**allegato 6**)
  1) Allegato I – ogni contraente inserisce i propri dati
  2) Allegato II – lo compila ASST oppure lo compila il Responsabile e viene verificato dal Delegato
  3) Allegato III – il Responsabile autocertifica l'esistenza, presso la propria organizzazione, delle misure di sicurezza minime indicate, inderogabili per lo svolgimento del contratto di servizio/fornitura.
  4) Allegato IV – compilato dal Responsabile.

Per le ipotesi di nomine di Responsabili a carico di professionisti per attività di consulenza specialistica, qualora si configuri un trattamento dei dati, in capo a questi ultimi, di titolarità di ASST, si fa riferimento al format di cui **all'allegato 7,** anche come parte dello stesso contratto principale, qualora possibile.
I Delegati al trattamento dei dati di cui al punto 2.3, dell'area amministrativa, sono altresì delegati alla sottoscrizione della nomina di Responsabile del trattamento quando prevista nell'ambito delle loro funzioni.

2.8 Attività di prova/sperimentazione di dispositivi/apparecchiature - Qualora, per le attività di prova di un dispositivo medico e/o apparecchiature elettromedicali, il potenziale fornitore sia nelle condizioni di svolgere trattamenti di dati di titolarità della ASST, vengono messe in atto le procedure di cui alla MAS14 che includono, dove necessario, l'utilizzo del modello di nomina di Responsabile del trattamento di cui al punto 2.7 (**allegato 6**), così come approvato nel presente regolamento e impegnano il potenziale fornitore in virtù della sottoscrizione della MAS14 e dei documenti sottoscritti che è tenuto ad allegare, come descritto nella procedura. In caso di assegnazione di incarico/ordine al fornitore l'azienda farà valere i termini dell'accordo precedentemente sottoscritti dal fornitore come Responsabile del trattamento.
La stessa procedura sarà messa in atto qualora la "prova" venga effettuata con applicativi e software informatici, pertanto il Delegato responsabile dell'attivazione della prova acquisirà dal fornitore l'impegno di seguito indicato (già contenuto nella MAS14 di cui sopra) oltre al modello di nomina di Responsabile del trattamento debitamente sottoscritto, in analogia con la procedura relativa ai dispositivi medici.
"Codesta spettabile Ditta assume l'impegno di rispettare i principi generali e i compiti particolari propri del Responsabile Esterno del trattamento dei dati, la cui titolarità è in capo all'ASST Ovest Milanese. I compiti in carico al Responsabile del trattamento sono indicati nel contratto di nomina di Responsabile del trattamento allegato alla presente ed ivi richiamato, con impegno di compilazione

degli ulteriori allegati annessi, nel rispetto di quanto indicato all'art 28 c. 1 del Reg UE 679/2016. Al termine del periodo di prova, la Ditta fornitrice si impegna a cancellare tutti i dati riferibile ai pazienti. Prima della cancellazione, se richiesto dal personale sanitario, i dati dovranno essere copiati su supporto informatico e messi a disposizione dell'ASST".
I Delegati responsabili valutano la necessità di acquisire una preventiva DPIA in base all'ipotesi di legge.

2.9 "Contitolari del trattamento" (art. 26 del Reg. UE 2016/679) – Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui 13 e 14 del Reg. UE 2016/679, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contenuti con gli interessati. L'accordo di contitolarità può essere messo a disposizione dell'interessato su richiesta dello stesso. Tale accordo deve disciplinare necessariamente almeno i seguenti contenuti: 1. Ambito di trattamento (oggetto, finalità); 2. Gestione delle informative; 3. Esercizio dei diritti; 4. Gestione data breach. Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

2.10 Collaborazioni istituzionali e rapporti convenzionali (con altre ASST/Istituti di formazione/altri Enti e soggetti vari) - Si esemplificano di seguito le ipotesi, non esaustive, ma ricorrenti, di rapporti convenzionali stipulati dalla ASST Ovest Milanese, tenuto conto comunque della necessità di analizzare, di volta in volta, in modo puntuale, l'oggetto della convenzione per definirne i ruoli:

- Convenzioni con altre ASST per lo svolgimento di attività di cura da parte delle altre ASST a supporto della ASST Ovest Milanese e viceversa, della ASST Ovest Milanese a supporto delle altre ASST: nell'ambito del rapporto convenzionale sono Responsabili del trattamento le ASST che mettono al servizio delle altre le proprie competenze;
- Convenzione con Enti aventi competenze e finalità istituzionali differenziate nell'ambito delle quali si svolgono congiuntamente o meno gli stessi trattamenti. In questo caso si hanno le ipotesi di Titolari autonomi o Contitolari;
- Convenzioni con istituti scolastici e di formazione per tirocini. In questo caso le parti assumono il ruolo di Titolari autonomi (vedi anche punto 2.4 e **allegato 3**);
- Incarichi ad avvocati per conferire loro il mandato di esercizio dell'attività giudiziaria. In questo caso le parti assumono il ruolo di Titolari autonomi. Nel caso in cui ad un avvocato venga dato un incarico di mera consulenza, nel rapporto giuridico, il ruolo di quest'ultimo si configura come Responsabile del trattamento (vedi punto 2.7 e **allegato 7**)

2.11 "Gruppo di lavoro aziendale in materia di privacy" - Il gruppo di lavoro è composto dalle figure aziendali che rappresentano le funzioni trasversali necessarie agli adempimenti normativi privacy ed è costituito con Deliberazione del Direttore Generale. Ha una funzione consultiva e consente all'organizzazione, titolare del trattamento, di valutare in modo multidisciplinare i rischi connessi alla gestione dei dati personali e le azioni di miglioramento che si intendono perseguire. Al fine di un'efficace organizzazione delle attività, è prevista la possibilità di lavorare anche in gruppi ristretti, in base agli argomenti oggetto di confronto e, in ogni caso, il Responsabile della Protezione dei Dati si riserva di invitare al gruppo di lavoro tutti coloro che di volta in volta fossero coinvolti dalle attività in essere (sia strutture di parte sanitaria che di parte amministrativa).

2.12 "Gruppo di valutazione delle violazioni" – Il gruppo di valutazione è lo strumento organizzativo attraverso cui vengono istruite le violazioni segnalate dai delegati o mediante "reclamo" dagli utenti.
L'attività del gruppo di valutazione è disciplinata dal Regolamento aziendale (di cui al punto 8) per la gestione del procedimento di notifica al Garante per la protezione dei dati di un "data breach".

3. PRINCIPIO DI LICEITA'

L'ASST Ovest Milanese tratta i dati personali dei soggetti interessati osservando i seguenti presupposti giuridici:

- Art. 6 Reg. UE 2016/679

1) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte (art. 6.1 lett. b) del Reg. UE 2016/679);
2) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6.1 lett. c) del Reg. UE 2016/679);
3) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato (art. 6.1 lett. d) del Reg. UE 2016/679);
4) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6.1 lett. e) del Reg. UE 2016/679)

- Art. 9 Reg. UE 2016/679

1) il trattamento è necessario per tutelare un interesse vitale dell'interessato (art. 9.2 lett. c) del Reg. UE 2016/679);
2) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria (art. 9.2 letr. f) del Reg. UE 2016/679);
3) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati Membri (art. 9.2 lett. g) del Reg. UE 2016/679);
4) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali ("finalità di cura") - art. 9.2 lett. h) del Reg. UE 2016/679;
5) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare) – Art. 9.2 lett. i) del Reg. UE 2016/679;
6) il trattamento è necessario a fini di archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici (art. 9.2 lett. j) del Reg. UE 2016/679).

Dove non vengano soddisfatti i suddetti presupposti giuridici l'Azienda valuta se il trattamento dei dati che si intende mettere in atto possa trovare fondamento nell'espressione del consenso dell'interessato, osservando i principi del GDPR e le indicazioni contenute nei provvedimenti del Garante.
Il consenso deve essere una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che dati personali che lo riguardano siano oggetto di trattamento.
Non dovrebbe mai, pertanto, configurare consenso il silenzio, l'inattività o la preselezione di caselle.

4. PRINCIPIO DI TRASPARENZA

4.1 INFORMATIVA

L'ASST Ovest Milanese fornisce agli interessati tutte le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679 tramite documenti, codificati dalla S.C Qualità e Risk Management, redatti in forma concisa e trasparente, con un linguaggio semplice e chiaro, seguendo le indicazioni contenute nelle Istruzioni operative aziendale IAP106.
Le informative, declinate in forma generale e in forma più specifica per alcune attività, sono pubblicate nella sezione "privacy" del sito istituzionale, nell'intranet aziendale, nello spazio Qweb e nei punti di informazione dell'ASST. Nei punti di maggiore affluenza del pubblico e di accoglienza sono affisse le informative di carattere generale e quelle più specifiche se di riferimento alle attività istituzionali dello specifico luogo di accesso.

4.2 INFORMATIVA BREVE PER IL TRATTAMENTO DEI DATI MEDIANTE L'UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Al fine di rendere l'informazione sul trattamento dei dati agli interlocutori delle mail scambiate nell'ambito dell'attività lavorativa, si invita il personale all'utilizzo del format sottostante da apporre, in modalità automatica, in calce alle mail aziendali:

"I vostri dati, di cui l'indirizzo mail, sono trattati in via informatica nel rispetto dei principi di protezione della privacy ed esclusivamente per soddisfare l'oggetto della mail, il cui contenuto, di carattere aziendale e non personale, è trasferibile all'interno dell'organizzazione di ASST. Si potranno comunque sempre esercitare i diritti di cui al capo III del Regolamento UE 2016/679 (accesso, correzione, cancellazione, opposizione al trattamento ecc). Il contenuto di questo messaggio è strettamente riservato al destinatario e qualora, per errore di trasmissione, pervenisse a persona diversa, preghiamo di contattarci immediatamente, avvertendo che la ritenzione, l'uso indebito e la diffusione non espressamente autorizzata della comunicazione potranno comportare la violazione della normativa sulla privacy".

4.3 DIRITTI DELL'INTERESSATO

L'interessato può esercitare tutti i diritti previsti dall'art. 15 e seg. del Reg, UE 2016/679 (il diritto all' accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione al trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, nonché il diritto di revoca del consenso qualora previsto. L'esercizio di tali diritti è valutato tenendo conto:

- dei vincoli di conservazione della documentazione secondo quanto stabilito dal Massimario di scarto regionale
- degli obblighi di legge
- della necessità di tutelare la privacy di eventuali controinteressati
- altri interessi pubblici rilevanti da contemperare rispetto al diritto della privacy

Per l'esercizio di tali diritti l'utente può utilizzare l'apposito modulo scaricabile dal sito web aziendale o reperibile presso l'Ufficio Relazioni col Pubblico (URP) e in ogni caso attraverso i dati di contatto del Titolare del trattamento e del DPO indicati nelle informative aziendali.
Alla richiesta di esercizio dei diritti verrà dato riscontro entro 30 giorni, con eventuale possibilità di proroga di altri 30 giorni ai sensi di legge. L'interessato può proporre reclamo all'Autorità del Garante o adire le opportune Autorità Giudiziarie in caso di violazioni.
Al fine di identificare sempre l'interessato che esercita i diritti previsti dall'art. 15 e seg., sarà chiesto a quest'ultimo di produrre copia di un documento di riconoscimento in corso di validità (DPR 445/00).
Il DPO supporta il Titolare del Trattamento, nella formulazione delle risposte, sentiti i Delegati interessati e il Responsabile SIA quando necessario. A tal fine è autorizzato ad istruire e approfondire raccogliendo tutte le informazioni necessarie alla corretta formulazione della proposta di risposta; i Delegati del trattamento si rendono disponibili per qualunque confronto.
Il DPO si interfaccia direttamente con l'interessato per eventuali risposte interlocutorie e/o di integrazione istruttoria.
In caso di richiesta di rettifica dei dati da parte dell'interessato l'istanza viene assegnata alla struttura che gestisce i dati con l'obbligo di darne riscontro all'interessato stesso.
Per quanto riguarda l'esercizio del diritto alla revoca del consenso, nei casi previsti, la manifestazione di tale volontà viene rivolta direttamente alla struttura che ha raccolto il consenso, al fine di tenerne conto nella gestione dei trattamenti in essere, previo l'obbligo di conservare agli atti la dichiarazione come predisposto nei modelli aziendali.
L'interessato può presentare reclamo nel caso ritenga violato il suo diritto alla privacy. Il DPO supporta il titolare nella gestione del reclamo che pervenga in Azienda attraverso i canali di comunicazione esistenti. Pertanto è essenziale la tempestiva segnalazione da parte delle strutture riceventi.

5. REGISTRO DEI TRATTAMENTI

Il Titolare tiene il Registro delle attività di trattamento, di cui all'articolo 30 del Regolamento UE 2016/679.
Il Registro viene periodicamente aggiornato con la richiesta ai Delegati delle informazioni necessarie mediante la compilazione di un modello contenente i campi obbligatori per la compilazione del Registro. Per la compilazione e l'aggiornamento del Registro, qualora necessario, può essere coinvolto anche il Gruppo di lavoro aziendale, coordinato dal Responsabile della Protezione dei Dati.

Il Registro è approvato e sottoscritto dal Titolare del trattamento nella persona del rappresentante legale.
Il Registro è un documento interno la cui accessibilità è consentita alla Direzione strategica, ai Delegati del trattamento e al DPO, mediante cartella condivisa posta nell'intranet aziendale.

5.1 REGISTRO DEI TRATTAMENTI QUANDO ASST OVEST MILANESE È RESPONSABILE

Qualora l'Azienda assuma il ruolo di Responsabile del trattamento, è tenuta a redigere il Registro come Responsabili contenente tutte le categorie di attività relative al trattamento svolte per conto di altri Titolari del trattamento (art. 30 c. 2 Reg. UE 2016/679). Anche tale Registro viene posto in una cartella interna alla rete aziendale.

5.2 REGISTRO DEL MEDICO COMPETENTE

Chi in azienda svolge il ruolo di Medico Competente sia un dipendente che un soggetto esterno è tenuto alla redazione di un Registro del trattamento in qualità di Titolare come indicato nel provvedimento del Garante per la protezione dei dati (Doc-web n. 9585367 del 14/05/2021).

6. FORMAZIONE

Nel piano annuale di formazione aziendale, viene programmata dal DPO l'attività formativa obbligatoria, anche con l'ausilio di docenti esterni, in materia di privacy rivolta ai dipendenti, in modalità differenti: generalizzata con contenuti rivolti a tutti i dipendenti e/o mirata con contenuti differenziati in base a ruoli e figure privacy e a differenti categorie professionali, di cui al punto 2 del presente regolamento. Le lezioni possono svolgersi in modalità FAD o in aula.

7. SICUREZZA DEI DATI PERSONALI

7.1 MISURE ORGANIZZATIVE

Le indicazioni seguenti sono istruzioni e indicazioni sui comportamenti corretti da tenere e rappresentano le misure organizzative rivolte a tutti gli operatori per lo svolgimento delle attività amministrative e cliniche, al fine di contenere il rischio di episodi di violazioni alla privacy. Tali misure non riguardano il tema della sicurezza informatica, le cui policy sono previste da altro regolamento aziendale.

7.1.1 Esattezza e completezza dei dati

Occorre prestare la massima attenzione alla digitazione ed alla scrittura manuale di dati identificativi, facendo il possibile per evitare errori di battitura o di scrittura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo.
È importante, negli ambiti di responsabilità delle strutture:

- attivare delle misure di controllo sulla completezza e correttezza dei dati registrati chiedendo all'occorrenza una verifica con il soggetto interessato.
- verificare periodicamente i dati di contatto nelle anagrafiche dei pazienti, fornitori, utenti al fine di scongiurare il rischio di errate comunicazioni.

7.1.2 Scanner

Gli autorizzati che utilizzano lo scanner devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati.
Nel caso di apparecchi condivisi fra diversi uffici, occorre prestare attenzione affinché il documento digitalizzato venga inviato alla cartella gestita da autorizzati al trattamento.
In caso di errore di selezione del destinatario è necessario chiedere al collega l'immediata cancellazione del documento inviato.

7.1.3 Archivi cartacei

In ASST sono presenti numerosi archivi cartacei.
I documenti o gli atti che contengono dati personali devono essere contenuti in armadi, schedari e contenitori ad accesso controllato, muniti di serratura o riposti in locali con porta dotata di serratura.

Gli archivi o gli uffici devono essere sempre chiusi a chiave qualora non siano presidiati dal personale autorizzato.
Le copie delle chiavi devono essere in numero minimo e riconducibili alle sole persone autorizzate al trattamento, per garantire l'accesso solo agli autorizzati al trattamento.
Le chiavi devono essere custodite con diligenza e non in prossimità dell'armadio o del locale.
Ogni struttura ha la responsabilità di definire il responsabile della custodia delle chiavi in caso di dimissioni del lavoratore.
Inoltre le persone autorizzate:
- contribuiscono a garantire e perfezionare le misure di accesso ai locali e le misure di sicurezza contro il rischio di intrusione;
- accedono ai dati che siano strettamente necessari all'esercizio delle proprie funzioni e competenze;
- custodiscono gli atti e i documenti durante il trattamento e li restituiscono o li ricollocano nel posto dal quale li avevano prelevati, al termine delle operazioni;
- prestano attenzione a non lasciare pratiche e fascicoli in gestione incustoditi sulla scrivania, soprattutto se contenenti dati personali;
- prestano, nell'ipotesi di stampante usata da più persone, attenzione a non lasciare incustodite le stampe contenenti dati personali;
È necessario, prima di gettare la documentazione nel cestino della carta, provvedere a renderne non comprensibile il contenuto, anche utilizzando apparati distruggi documenti o altri più banali accorgimenti come ad esempio lo strappo dei documenti, la separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc.
È vietato stoccare documenti cartacei per terra. I prelievi degli archivi storici devono essere sempre documentati.

7.1.4 Spedizione di documenti a mezzo posta
La documentazione contenente dati personali movimentata con posta interna deve essere trasferita in busta chiusa e sigillata, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti.

7.1.5 Utilizzo del fax
Il Fax è un mezzo obsoleto di trasmissione di dati e documenti, perché non è garantita la consegna direttamente al destinatario dei documenti che vengono inviati.
Nei casi in cui non sia possibile trasmettere i dati con altri strumenti (applicativi, mail, pec, raccomandata, busta chiusa a mano) è consentito l'utilizzo del fax, nel rispetto di alcune misure di sicurezza:
- in calce ai fax trasmessi dall'ASST Ovest Milanese, sia all'interno che all'esterno, deve essere posta la seguente dicitura:

Il contenuto del presente fax ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione.
Se il fax e i suoi allegati sono stati ricevuti per errore da persona diversa dal destinatario siete pregati di distruggere tutto quanto ricevuto e di informare il mittente ai numeri telefonici indicati.

- prima di inviare un fax, l'operatore inviante deve avvisare della spedizione e quindi accertarsi che il destinatario sia nella condizione di poter ritirare rapidamente il documento stampato;
- l'apparecchio che riceve il documento deve essere allocato in un locale non aperto al pubblico, al quale possono accedere solo gli autorizzati al trattamento dei dati trasmessi;
- le comunicazioni ricevute via fax non devono essere lasciate incustodite e visibili a terzi ed immediatamente prese in carico dall'autorizzato.

7.1.6 Sportelli
Per garantire la riservatezza dei colloqui, presso gli sportelli o gli ambulatori devono essere previsti appositi spazi, segnalati con una riga gialla oltre i quali gli utenti possano attendere il proprio turno.
I nomi dei pazienti in attesa di una prestazione o di documentazione (ad esempio delle analisi cliniche) non devono essere divulgati ad alta voce. Si suggerisce l'attribuzione un codice alfanumerico al momento della prenotazione o accettazione.

7.1.7 Luoghi di cura
Nei reparti dove si possono visitare i degenti solo attraverso vetrate (ad esempio reparto di rianimazione) devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino la visibilità dell´interessato durante l´orario di visita ai soli familiari e conoscenti.
Il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate.
Non devono essere affisse liste di pazienti ricoverati o in attesa di prestazione in locali aperti al pubblico, con o senza la descrizione della patologia sofferta.
Non devono essere resi visibili ad estranei documenti sulle condizioni cliniche del malato (ad esempio lasciando le cartelle cliniche vicino al letto di degenza).

7.1.8 Colloqui
È doveroso adottare idonee cautele in relazione allo svolgimento di colloqui (ad esempio in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell´interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.
Gli operatori ricevono cittadini e utenti, rimanendo sempre presenti nel proprio ufficio o luogo di lavoro, avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi, ad esempio rivoltando le cartelle o evitando di riportare sul frontespizio delle stesse, dati ed informazioni che permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento.

7.1.9 Telefoni
È assolutamente necessario non fornire per mezzo telefono dati ed informazioni di carattere sanitario o di natura comunque riservata qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante.
Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere il nome e qualità dell'interlocutore al fine di richiamarlo successivamente dopo aver ottenuto certezze sulla identità.

7.1.10 Consegna referti
I referti diagnostici, le cartelle cliniche, i risultati delle analisi e i certificati rilasciati dagli organismi sanitari possono essere consegnati in busta chiusa anche a persone diverse dai diretti interessati purché munite di delega scritta.
L'Interessato (cioè l'utente) deve presentare il modulo per il ritiro referti ed identificarsi con l'esibizione di un documento di identità.
L'eventuale delegato al ritiro dei referti deve presentare il modulo predisposto unitamente alla delega dell'interessato ed alla copia del documento di identità del delegante ed esibire del proprio documento di identità. Se sussistono difficoltà nell'acquisire la copia del documento di identità devono essere trascritti sul modulo ritiro referti gli estremi identificativi dei documenti di identità sia del delegato sia del delegante.
Il ritiro di un referto di minore deve essere preceduto da autocertificazione del genitore che attesta di essere genitore oppure accompagnato da una delega se persona diversa dal genitore come da modulistica in uso.

Per quanto riguarda i referti HIV, ai sensi dell'art. 5 c. 4 L. 135/90, la comunicazione dei risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti.
Inoltre, le linee guida del Garante in tema di referti online del 19 novembre 2009, fanno ritenere esclusa tale modalità di refertazione per l'esigenza di una specifica attività di consulenza da parte del personale medico, sia per i referti HIV che per i test genetici.

In ASST è consentita la refertazione online, come descritto nell'ambito dell'informativa MAC535 e corrispettivo modulo di consenso MAC535.1.

7.1.11 Comunicazioni a terzi

Le informazioni ai familiari e conoscenti possono essere fornite solo su espressa indicazione del paziente, se cosciente e capace.
Il personale autorizzato deve accertare l'identità dei terzi legittimati a ricevere le informazioni, avvalendosi anche di elementi desunti dall'interessato.
Occorre rispettare l'eventuale richiesta della persona assistita a non rendere note a terzi la propria presenza in ASST o le informazioni sulle sue condizioni di salute.
A tal fine l'ASST, in caso di degenza, raccoglie l'indicazione dei soggetti terzi a cui poter fare comunicazioni sullo stato di salute del paziente mediante l'uso della modulistica a tal fine codificata.
Qualora l'attività di cura non sia svolta in degenza, è in uso il modello MAC511 per la raccolta delle indicazioni di cui sopra da parte del paziente/utente.

8. VIOLAZIONE DI DATI – DATA BREACH

Il Titolare, nel valutare l'adeguato livello di sicurezza, tiene conto in special modo dei rischi presentati dai trattamenti, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. In caso di violazione ASST Ovest Milanese applica il Regolamento aziendale vigente.

9. VIDEOSORVEGLIANZA

Per gli aspetti di tutela dei dati di titolarità dell'ASST Ovest Milanese, si rinvia al regolamento aziendale vigente e alla relativa modulistica approvata.

10. DPIA

La valutazione di impatto (DPIA) viene svolta in azienda secondo quanto definito in apposita istruzione operativa codificata dalla S.C Qualità e Risk Management.

11. SPERIMENTAZIONI CLINICHE

Si rimanda al regolamento aziendale per la definizione dei ruoli privacy dei soggetti interni ed esterni coinvolti nelle attività di sperimentazione e per le informazioni da rendere agli interessati (pazienti che aderiscono ai progetti di ricerca).

12. SICUREZZA INFORMATICA

Per quanto riguarda il tema della sicurezza informatica, si rimanda al regolamento aziendale per l'utilizzo dei sistemi informatici (ad es. utilizzo di personal computer, pc portatili, smartphone ecc) che il personale è tenuto ad osservare.

13. REGOLAMENTO DONAZIONI

Si rimanda alla delibera n. 282 del 01/07/2022 "approvazione del regolamento delle donazioni" per la disciplina di eventuali valutazioni che attengono il trattamento dei dati di titolarità dell'ASST Ovest Milanese nelle ipotesi di donazioni di specifici beni o servizi.

Gent.mo/a Dott./Dott.ssa
(Nome Cognome)

Responsabile/Direttore
(Unità Operativa)

IN LUOGO

Oggetto: Delega alle attività di trattamento

In base al Reg UE 2016/679, in qualità di rappresentante legale della ASST Ovest Milanese, Titolare del Trattamento dei dati, in virtù dell'incarico di Responsabile/Direttore della UOC …… dell'ASST, Le affido lo svolgimento delle attività di trattamento dei dati di seguito indicate in qualità di Delegato.
Per Regolamento aziendale, il Titolare delega alle attività di trattamento sotto indicate tutti coloro che ricoprono incarichi di Direttore di Unità Operativa Complessa, di Responsabile di Unità Operativa Semplice Dipartimentale, di Responsabile di Unità Operativa Semplice di Staff della Direzione Strategica, nonché di Responsabile delle specifiche funzioni assegnate agli Staff della Direzione Strategica.
La delega conferita si riferisce ai trattamenti di tutti i dati (comprese le categorie particolari di dati) che attengono alle attività rese ai pazienti e agli utenti ed effettuate nell'ambito di Sua competenza. Tale attività ha durata per tutto il periodo di assunzione del Suo incarico ed è da considerarsi confermata con il rinnovo dell'incarico stesso a seguito di valutazione positiva, quando prevista.

Il Delegato è pertanto tenuto a:

1. accertarsi che il trattamento dei dati nell'ambito della propria UOC sia preceduto da una corretta informazione all'utente, avvalendosi dei modelli e delle procedure predisposti dall'azienda;
2. provvedere, su richiesta dell'interessato, ad aggiornare e/o modificare, i dati dello stesso, laddove possibile, nell'ambito della sua capacità organizzativa;
3. segnalare al Titolare del trattamento eventuali reclami da parte di terzi e informare di qualunque fatto che possa compromettere la sicurezza dei dati;
4. garantire il rispetto della normativa in materia di tutela dei dati personali, anche sotto il profilo delle misure di sicurezza, attenendosi alle misure tecniche ed organizzative previste dai regolamenti aziendali;
5. richiedere l'accesso a sistemi ed applicativi in uso presso la propria struttura per i dipendenti che rientrano nell'ambito della propria competenza organizzativa e richiederne la disabilitazione in caso di trasferimento interno all'ASST, secondo quanto indicato nel "Regolamento aziendale per l'utilizzo dei sistemi informativi ai sensi dell'art. 32 del regolamento UE 2016/679".
6. accertarsi che le persone autorizzate a trattare i dati nel Suo ambito organizzativo operino in conformità alle istruzioni ricevute dal Titolare e alle misure tecniche ed organizzative adottate in azienda. A tal proposito Lei è delegato a conferire più specifiche istruzioni se necessarie e a fornirle anche ai soggetti esterni autorizzati ai trattamenti (ad es. personale volontario, studenti ecc.);
7. nominare gli Amministratori di sistema che operano all'interno della propria struttura, qualora esistenti, mediante il modello in uso ed esercitare un controllo sulle attività degli stessi per la sicurezza dei data base a loro affidati;
8. comunicare immediatamente al Titolare del trattamento eventuali nuovi trattamenti da intraprendere valutando la necessità di procedere con una DPIA (valutazione d'impatto ex art. 35 Reg. UE 2018/679) secondo le modalità indicate nella specifica istruzione Aziendale;

9. collaborare con il Titolare per tutti gli adempimenti attribuiti a quest'ultimo nel Regolamento UE, compresa la redazione del Registro dei trattamenti (quando coinvolto dal Titolare e dal Responsabile della Protezione dei Dati);
10. collaborare con il Titolare e il Responsabile della Protezione dei Dati aziendale per tutte le necessità, in particolare per le segnalazioni di Data Breach, nell'ambito del gruppo di valutazione previsto nel Regolamento vigente, nonché per evadere tempestivamente eventuali richieste di informazioni da parte dell'Autorità Garante e dare immediata esecuzione alle indicazioni della stessa Autorità.
11. A fronte die rischi specifici in materia di privacy nel proprio settore/reparto, il delegato è tenuto a definire misure organizzative e concordare con il SIA e/o ingegneria clinica eventuali misure tecniche a tutela della sicurezza dei dati personali. Le misure definite devono essere condivise con il personale sottoposto e tale attività informativa/formativa deve essere documentata. In fase di indagine dei rischi il delegato collabora nel processo di rendicontazione delle misure già predisposte e segnala situazioni a rischio per stabilire per tempo opportune situazioni di miglioramento.

Cordiali saluti.

Legnano,

Il Direttore Generale
Titolare del Trattamento
Dott. Fulvio Edoardo Odinolfi

Data e luogo_____

Firma per accettazione_____

Al Sig./Alla Sig.ra
(Nome Cognome)
(Unità Operativa)

IN LUOGO

Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative

Con la presente Le comunico che, per le funzioni a Lei attribuite, nell'ambito della struttura di riferimento, è autorizzato al trattamento dei dati personali (comprese le categorie particolari) riguardanti le attività descritte nella scheda del Registro aziendale afferente alla Sua struttura di appartenenza, anche mediante l'uso dei sistemi ICT per i quali sono state chieste apposite credenziali di accesso a suo esclusivo uso personale, non cedibili ad altro utente e funzionali esclusivamente alla prestazione delle attività ivi attribuite.
Per consentirLe di operare in modo corretto è necessario che si attenga alle seguenti informazioni di carattere generale.
Dovrà operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali coperti da riservatezza, non potendo divulgare a terzi le informazioni di cui ha conoscenza anche successivamente all'incarico svolto.
I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che Le vengono assegnate, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito quando la conoscenza è strettamente necessaria allo svolgimento delle attività.
I dati dovranno essere custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.
Per una completa informazione circa i comportamenti da tenere Lei è invitato a visionare i regolamenti aziendali vigenti riguardanti le misure di sicurezza tecniche ed organizzative e a rispettare le disposizioni ivi contenute.
In ogni caso Lei è tenuto al rispetto delle specifiche ed ulteriori istruzioni fornite dal Responsabile, delegato dal Titolare, individuato in ASST nel Direttore di UOC, nel Responsabile di UOSD, nel Responsabile di UOS di Staff, nonché nel Responsabile di specifiche funzioni assegnate agli Staff della Direzione Strategica.
La presente autorizzazione al trattamento è limitata esclusivamente alla sussistenza del rapporto di lavoro dipendente in generale ed in particolare presso la struttura di attuale assegnazione.

Le segnalo in sintesi le principali istruzioni operative, già contenute nella descrizione delle misure di sicurezza dei Regolamenti aziendali.

1) TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone estranee al trattamento.
- I documenti contenenti dati personali devono essere conservati in contenitori o locali muniti di serratura.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie e tavoli di lavoro e i documenti che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- Devono essere distrutte le copie di stampa che per il particolare contenuto di riservatezza, non si prestano al riuso per bozze.

2) TRATTAMENTI CON STRUMENTI ELETTRONICI

Gli autorizzati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Le password devono essere mantenute riservate.
- Username e password non devono mai essere condivise tra più soggetti. Nel caso in cui altri utenti debbano poter accedere ai dati è necessario richiedere credenziali aggiuntive.
- Le password sono sostituite periodicamente in base alle istruzioni contenute nel Regolamento aziendale per l'utilizzo dei Sistemi Informativi Aziendali.

- Non devono essere lasciate incustodite le postazioni di lavoro durante una sessione di trattamento senza avere preventivamente bloccato il PC o disconnesso l'utenza (premere contemporaneamente i tasti CTRL + ALT + CANC e selezionare l'opzione "blocca computer" o "Disconnetti").

Cordiali saluti

Legnano, *(data)*

Titolare del trattamento
Il Direttore Generale

Al Sig./Alla Sig.ra
(Nome Cognome)

IN LUOGO

Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative

Con la presente Le comunico che, è autorizzato al trattamento dei dati personali (comprese le categorie particolari) per le funzioni a Lei attribuite nell'ambito dell'accordo assunto tra l'ASST e il Suo Ente di provenienza (attività di tirocinio, alternanza scuola-lavoro, volontariato).

Per lo svolgimento della Sua attività, è stato abilitato all'uso dei seguenti applicativi:

- (nome applicativo)
- (nome applicativo)
  oppure
- (NESSUN APPLICATIVO)

e all'accesso alle seguenti informazioni:

- (nome banca dati)
- (archivi)
- (notizie acquisite in reparto/uffici)

Per consentirLe di operare in modo corretto è necessario che si attenga alle seguenti indicazioni di carattere generale.

Dovrà infatti operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali coperti da segretezza, non potendo divulgare a terzi le informazioni di cui viene a conoscenza anche successivamente all'incarico svolto.
I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che Le vengono assegnate, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito quando la conoscenza è strettamente necessaria allo svolgimento delle attività.
I dati dovranno essere custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

Lei è tenuto al rispetto delle istruzioni fornite dal Delegato del Titolare, anche per il tramite del Suo Tutor, qualora presente.

Le segnalo in sintesi le principali istruzioni operative, già contenute nella descrizione delle misure di sicurezza dei Regolamenti aziendali.

3) TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento.
- I documenti contenenti dati personali devono essere conservati in contenitori o locali muniti di serratura.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie e tavoli di lavoro e i documenti che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

- Devono essere distrutte le copie di stampa che per il particolare contenuto di riservatezza, non si prestano al riuso per bozze.

4) TRATTAMENTI CON STRUMENTI ELETTRONICI

- Gli incaricati devono utilizzare e gestire le proprie credenziali di autenticazione con diligenza.
- Le password devono essere mantenute riservate. Username e password non devono mai essere condivise tra più soggetti. Nel caso in cui altri utenti debbano poter accedere ai dati è necessario richiedere credenziali aggiuntive.
- Le password sono sostituite periodicamente in base alle istruzioni contenute nel Regolamento aziendale per l'utilizzo dei Sistemi Informativi Aziendali.
- Non devono essere lasciate incustodite le postazioni di lavoro durante una sessione di trattamento senza avere preventivamente bloccato il PC o disconnesso l'utenza (premere contemporaneamente i tasti CTRL + ALT + CANC e selezionare l'opzione "blocca computer" o "Disconnetti").

Cordiali saluti

Legnano, *(data)*

Il Delegato del Titolare

_____

Per presa visione, l'autorizzato

_____

Al Sig./Alla Sig.ra
(Nome Cognome)
(Unità Operativa)

IN LUOGO

Oggetto: Nomina ad "Amministratore del sistema"

Il provvedimento del Garante per la protezione dei dati personali "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"** del 27 novembre 2008, aggiornato al 25 giugno 2009, definisce le caratteristiche e i compiti dell'Amministratore di sistema, che svolge attività particolarmente qualificate nell'ambito degli apparati di rete e per la sicurezza delle informazioni.
Pertanto, tenuto conto delle competenze tecniche, delle mansioni svolte e della sua assegnazione presso la UO Servizi Informativi Aziendali, con la presente viene nominato "**Amministratore di sistema**", nell'ambito di operatività delle sue funzioni di supporto tecnico, configurazione, installazione, sviluppo evolutivo e gestione progettuale di:
☐ sistemi software complessi e database di ambito sanitario
☐ sistemi software complessi e database di ambito amministrativo
☐ sistemi server, database, sistemi di sicurezza, reti di dati, servizi di base hardware e software

Si fa presente che il Provvedimento di cui sopra, obbliga l'Azienda alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza dei trattamenti dei dati eseguiti, alle misure organizzative, tecniche e di sicurezza.
Inoltre i suoi estremi identificativi e le funzioni correlate sono comunicate al Garante in caso di accertamenti e ai soggetti indicati al punto 4.3 del Provvedimento qualora si ravvisino le condizioni.

Cordiali saluti

Legnano, *(data)*

Delegato del Titolare

Luogo e data _____

Firma per accettazione

_____

Al Sig./Alla Sig.ra
(Nome Cognome)

IN LUOGO

Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative

Con la presente Le comunico che è autorizzato al trattamento dei dati personali (comprese le categorie particolari di dati), per le attività che Lei svolge in ASST nell'ambito delle attività definite nel "protocollo d'intesa per la promozione di strategie condivise finalizzate alla prevenzione e al contrasto del fenomeno della violenza nei confronti delle donne" del 28/11/2013 aggiornato il 14/7/2016.
Considerato che lo svolgimento della Sua attività, svolta presso l'Azienda, comporta l'acquisizione e la conoscenza di informazioni contenenti dati personali (comprese le categorie particolari di dati) di specifiche categorie di Pazienti, Le vengono fornite indicazioni operative atte a consentirLe il corretto operare nel rispetto alle disposizioni del Reg. UE 2016/679.
Dovrà pertanto garantire la massima riservatezza dei dati personali di cui viene a conoscenza, non potendo divulgare le informazioni acquisite, a terzi che non siano gli operatori autorizzati dell'ASST o della rete di cui ai protocolli sopracitati, anche al termine del Suo incarico, se non per obbligo di legge.
La comunicazione dei dati e delle informazioni dovrà pertanto avvenire secondo le modalità operative del contesto organizzativo dell'Azienda, mantenendo un ambito limitato e necessario di contatti con gli operatori.
I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che svolge, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito in quanto strettamente necessaria allo svolgimento delle attività.
I dati, nelle varie forme di trattamento, dovranno essere anche custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.
In ogni caso Lei è tenuto al rispetto di tutte Le eventuali ulteriori specifiche indicazioni fornite dal Delegato del Titolare.

Distinti saluti

Legnano, *(data)*

Delegato del Titolare

Per presa visione, l'autorizzato

_____

Spett.le

_____

Oggetto: Nomina di Responsabile del Trattamento dei dati del Trattamento a norma dell'art. 28 del Regolamento (UE) 2016/679

SEZIONE I

Articolo 1

SCOPO E AMBITO DI APPLICAZIONE

a) Scopo del presente accordo è garantire il rispetto dell'art. 28, paragrafo 3 e 4, 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)
b) I presenti articoli si applicano al trattamento dei dati personali specificato all'Allegato II
c) Gli allegati costituiscono parte integrante del presente atto
d) I presenti articoli lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del Regolamento (UE) 2016/679
e) I presenti articoli non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al Capo V del Regolamento UE 2016/679 ovvero sarà cura delle parti stabilire opportune garanzie ai sensi dell'art. 46 del Reg. UE.

Articolo 2

INVARIABILITÀ DEGLI ARTICOLI

a) Le parti si impegnano a non modificare gli articoli se non per aggiungere o aggiornare informazioni negli allegati.
b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nella presente nomina, in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Articolo 3

INTERPRETAZIONE

a) Quando i presenti articoli utilizzano i termini definiti, rispettivamente, nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al Regolamento interessato.
b) I presenti articoli vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679.
c) I presenti articoli non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

SEZIONE II

OBBLIGHI DELLE PARTI

Articolo 4

DESCRIZIONE DEL TRATTAMENTO

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'Allegato II.

Articolo 5

OBBLIGHI DELLE PARTI

5.1 Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento.
b) In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali.
c) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

5.2 Limitazione delle finalità

a) Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'Allegato II, salvo ulteriori istruzioni del titolare del trattamento.

5.3. Durata del trattamento dei dati personali

b) Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'Allegato II.

5.4 Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'Allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
b) Il responsabile individua per iscritto i soggetti autorizzati e definisce le attività operative degli stessi, per lo svolgimento delle mansioni loro affidate garantendo un corretto, lecito e sicuro trattamento dei dati nell'ambito del sistema informatico oltre che l'impegno alla riservatezza degli stessi incaricati, quale obbligo legale espressamente dichiarato. Il Responsabile rende disponibile, su richiesta del Titolare, l'elenco dei soggetti autorizzati al trattamento.
c) Con riferimento allo svolgimento delle attività attinenti la funzione di Amministratore di sistema, si indicano le seguenti attività di cui al provvedimento del Garante del 27/11/2008 aggiornato al 25/06/2009:
    - individuare, nell'ambito della propria organizzazione, la o le persone (dipendenti o collaboratori) munite dei necessari requisiti di esperienza, capacità ed affidabilità, cui attribuire, rispetto al sistema informatico aziendale del Titolare, le mansioni di amministratore di sistema definendone gli ambiti di operatività, in conformità al provvedimento 27 novembre 2008 (aggiornato al 2009) del Garante per la protezione dei dati personali;
    - conservare, aggiornare e mettere a disposizione del Titolare, l'elenco con i dati (nome, cognome, funzione) degli amministratori;
    - predisporre ed attuare un idoneo sistema di controllo periodico sull'operato dei propri amministratori, in particolare per la registrazione degli accessi logici, fornendo tutte le informazioni al Titolare sulla correttezza dell'attività di queste persone rispetto alle misure di sicurezza adottate ed alle mansioni attribuite.
    - Il Responsabile, qualora possibile, aderirà ai codici di condotta o alle certificazioni di cui agli artt. 40-42 del Reg. UE 2016/679.

5.5 Dati sensibili

a) Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari stabilite dal

Comitato Europeo e, nello specifico, dall'Autorità Garante Nazionale mediante D.lgs 196/13 aggiornato dal D.lgs 101/18 e provvedimenti tempo per tempo vigenti.

5.6 Documentazione e Rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole contrattuali.
b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di verifica delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito alle modalità di verifica, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.
d) Il titolare del trattamento può scegliere di condurre l'attività di controllo autonomamente o incaricare un auditor indipendente. Le attività di controllo possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui al presente articolo, compresi i risultati di eventuali attività di controllo.

5.7 Ricorso a sub-responsabili del trattamento

a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere all'elenco dei sub-responsabili del trattamento indicati nell'Allegato IV. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 20 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.
b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679.
c) Ai sensi dell'art. 28 c. 4, qualora il sub Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub Responsabile. Il Responsabile del trattamento nomina un sub Responsabile mediante atto scritto che contenga i medesimi obblighi tra Titolare e Responsabile, prevedendo garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate.
d) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
e) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.
f) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

5.8. Trasferimenti internazionali

a) Il Responsabile del trattamento non può comunicare, diffondere e trasferire i dati a soggetti terzi né, tantomeno, a Paesi terzi extra Unione Europea, senza l'autorizzazione del Titolare, salvo per adempiere

a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del Regolamento (UE) 2016/679.

b) Pertanto i dati saranno trattati all'interno dell'Unione Europea. Il Responsabile, che agisce al di fuori dell'Unione Europea, deve attenersi al rispetto delle procedure di verifica del livello di protezione dei dati, di cui al Capo V del Reg Ue 2016/679. Il Responsabile dovrà garantire e documentare, sotto la propria responsabilità, che nel Paese di importazione il livello di protezione dei dati è "sostanzialmente equivalente" a quello in vigore presso l'Unione europea, allineandosi alle procedure di cui alle Raccomandazioni di EDPB del 10/11/20.

c) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente all'articolo 5.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del Regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del Regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'art. 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

d) Le parti convengono che le garanzie per il trasferimento verso paesi terzi adottate ai sensi dell'art. 46 del Reg. UE 2016/679 dal responsabile e suoi sub-responsabili/contitolari vengano esibite in fase di sottoscrizione del presente accordo e allegate allo stesso.

Articolo 6

ASSISTENZA AL TITOLARE DEL TRATTAMENTO

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità dell'articolo 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

   1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
   2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

d) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

e) gli obblighi di cui all'articolo 32 Regolamento (UE) 2016/679;

f) Le parti stabiliscono nell'Allegato III le misure tecniche e organizzative minime (tenuto conto dei rischi cogenti e dei provvedimenti stabiliti dall'Autorità Garante all'atto della sottoscrizione del presente accordo) con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione del presente articolo, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Articolo 7

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli artt. 33 e 34 del Regolamento (UE) 2016/679 o degli artt. 34 e 35 del Regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

7.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'art. 33, par. 3, del Regolamento (UE) 2016/679/, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
    - la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    - le probabili conseguenze della violazione dei dati personali;
    - le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
    - le misure di mitigazione adottate dallo stesso responsabile del trattamento per prevenire e fronteggiare la violazione; nonché, se di propria competenza le misure di miglioramento per attenuarne nel futuro i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente entro 72 ore dalla segnalazione della violazione, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'art. 34 del Regolamento (UE) 2016/679/, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

7.2. Violazione riguardante dati trattati dal responsabile del trattamento

a) In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento entro 24 ore dopo esserne venuto a conoscenza. La notifica contiene almeno:

- una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

b) Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
c) L'Allegato III indica le misure di sicurezza minime che il Responsabile del trattamento è tenuto ad adottare in conformità con quanto stabilito dalla normativa vigente per la protezione dei dati personali.
d) Il Responsabile, oltre a quando già disposto all'art. 28 c. 10, è obbligato a tenere indenne il Titolare da ogni responsabilità, costo, spesa o altro onere, discendenti da pretese, azioni o procedimenti di terzi a causa della violazione, da parte del Responsabile (o di suoi dipendenti o collaboratori ovvero dei sub Responsabili), degli obblighi a suo carico in base alla presente e della violazione delle prescrizioni di cui alla vigente normativa in materia di protezione dei dati personali.

SEZIONE III

DISPOSIZIONI FINALI

Articolo 8

INOSSERVANZA DELLE CLAUSOLE CONTRATTUALI E RISOLUZIONE

a) Fatte salve le disposizioni del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole contrattuali, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole

o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

- il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
- il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725;
- il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità dell'articolo 5.1, lettera c), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

e) Gli eventuali oneri e spese derivanti dagli adempimenti della presente nomina sono a carico del Responsabile, a cui non corrisponde nessun diritto a compensi e rimborsi.

f) In nessun caso il Responsabile acquisisce la proprietà intellettuale dei dati e delle informazioni trattate nell'ambito dello svolgimento del contratto.

Data_____

Con i migliori saluti.

Il Delegato del Titolare al trattamento dei dati

Data_____

Per presa visione e accettazione

Il Legale Rappresentante della Società, quale Responsabile esterno del trattamento

_____

ALLEGATO I

Elenco delle parti

Titolare/i del trattamento: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1.Nome del Titolare del Trattamento _____

Nome e Cognome del Legale Rappresentante_____

Indirizzo della Sede Legale_____

CF/P.IVA_____

Dati di Contatto aziendali_____

Dati di Contatto del DPO_____

2.Responsabile/i del trattamento [Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

Nome del Responsabile del Trattamento _____

Nome e Cognome del Legale Rappresentante_____

Indirizzo della Sede Legale_____

SEDE DELLE OPERAZIONI DI TRATTAMENTO_____

CF/P.IVA_____

Dati di Contatto aziendali_____

Dati di Contatto del DPO_____

ALLEGATO II

Indicare con una X le voci che corrispondono agli ambiti di trattamento dei dati consentiti al Responsabile del Trattamento:

A) <u>Categorie di interessati i cui dati personali sono trattati</u>

- o Pazienti
- o Familiari/Care giver dei Pazienti
- o Utenti
- o Visitatori
- o Fornitori
- o Collaboratori/Dipendenti
- o Familiari dei Dipendenti
- o Volontari
- o Nessuno
- o Altro_____

B) <u>Categorie di dati:</u>

- o Dati Anagrafici
- o Contatti (es. telefono, mail)
- o Immagini
- o Dati economici (es. Coordinate Bancarie, Livello Retributivo, Premialità, Posizione Debitoria ecc)
- o Dati particolari/sensibili (riguardanti origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale)
- o Dati relativi alla salute
- o Dati Giudiziari
- o Dati Genetici
- o Dati Biometrici
- o Dati relativi agli accessi dell'interessato ai sistemi IT (es. log, indirizzo IP)
- o Nessuno
- o Altro_____

C) <u>Natura del trattamento:</u>

- o Raccolta
- o Registrazione
- o Organizzazione
- o Strutturazione
- o Conservazione
- o Adattamento o Modifica
- o Estrazione
- o Consultazione
- o Comunicazione
- o Nessuno
- o Altro_____

D) <u>Durata del Trattamento:</u>

- o Occasionale sino al termine del accordo
- o Sistematico sino al termine dell'accordo
- o Oltre al termine dell'accordo per soddisfare tale obbligo di legge _____ (*indicare i riferimenti di legge cui è soggetto il Responsabile del Trattamento*)
- o Nessuno

E) <u>Finalità per le quali i dati personali sono trattati per conto del titolare del Trattamento:</u>

<u>Oggetto della prestazione offerta ed estremi dell'atto di approvazione e/o del contratto di riferimento</u>

_____
_____
_____

<u>Modalità di accesso ai dati (es. da remoto, sul campo)</u>

_____
_____

<u>Motivazioni specifiche che rendono necessario il trattamento</u>

_____
_____
_____
_____
_____

ALLEGATO III

MISURE DI SICUREZZA MINIME

Di seguito sono elencate le misure di sicurezza minime volte a ridurre il verificarsi di eventi capaci di compromettere riservatezza, integrità e disponibilità dei dati personali trattati.

In qualità di Responsabile del trattamento è tenuto all'adempimento di tali misure in conformità con quanto stabilito dalla normativa privacy vigente (GDPR).

MISURE DI GESTIONE CONTROLLO DELLE POLITICHE PRIVACY
L'azienda ha stabilito un piano di disaster recovery e business continuity
L'azienda ha effettuato recentemente un'indagine sui rischi privacy
L'azienda dispone di un elenco degli Amministratori di Sistema e relativa mansione
L'azienda ha stabilito politiche che assicurano il controllo e riesame periodico delle misure stabilite a protezione dei dati personali
L'azienda ha stabilito delle misure per assicurare l'esercizio dei diritti degli interessati e pronta gestione dei reclami
L'azienda ha stabilito delle misure di controllo per assicurare il principio di minimizzazione dei trattamenti
L'azienda testa periodicamente l'efficacia del piano di disaster recovery e business continuity
L'azienda ha adottato un sistema di controllo che consente il trattamento SOLO sino al raggiungimento dei termini massimi di conservazione stabiliti
RISCHIO RISERVATEZZA
Sono stabilite misure volte a limitare l'accesso a personale non autorizzato agli spazi fisici
Sono stabilite misure volte a limitare l'accesso a personale non autorizzato alle banche dati digitali
L'azienda ha adottato sistemi di controllo automatici volti a limitare l'accesso ai locali in cui si effettua il trattamento
Esistono sistemi antivirus e firewall volti a bloccare tentativi di accesso non autorizzato dal web
Le banche dati in possesso dell'azienda sono cifrate
Il personale autorizzato è formalmente identificato e vi è evidenza delle istruzioni fornite
Sono stabilite misure per tracciare le operazioni effettuate da personale autorizzato
Le politiche di accesso stabilite sono verificate periodicamente
RISCHIO PERDITA E CANCELLAZIONE
Dove previsto l'affidamento di copia delle informazioni, esistono misure per testare l'efficacia delle procedure di backup stabilite
Dove previsto l'affidamento di copia delle informazioni, esistono misure per il ripristino di una copia dei dati affidati
Dove previsto l'affidamento di copia delle informazioni, esistono misure per assicurare la rintracciabilità delle informazioni

RISCHIO DI NON COMPLETA O CORRETTA COMPILAZIONE DEI DATI
Dove previsto dall'incarico, il personale adotta misure di controllo per assicurare la completa e corretta registrazione dei dati
Dove previsto dall'incarico, esistono delle forme di controllo indipendenti o effettuate da terze parti a garanzia della completezza e correttezza dei dati registrati

Presa visione della tabella, dichiara di adottare le misure qui sopra riportate e si rende disponibile a fornire eventuale evidenza degli adempimenti richiesti in ragione del contratto in essere con l'Azienda Titolare del Trattamento.

Data _____

Firma _____

ALLEGATO IV

A) <u>Elenco Sub-responsabili:</u>

Dati societari del Sub-Fornitore Incaricato	*Tipo di Trattamento affidato e Tipologia di dati trattati*		*Finalità del Trattamento*	*Sede del Trattamento*	*Sede Legale/ Sede Operativa*	*Modalità di Accesso ai dati (es. da remoto/sul campo)*

Spett.le

_____

Oggetto: Nomina di Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE 2016/679.

In riferimento agli accordi in essere, regolati da contratto o convenzione (*indicare l'oggetto e gli estremi dell'atto di approvazione e/o del contratto di riferimento)*, il Titolare del Trattamento di dati personali, nella persona di rappresentante legale o di suo delegato, La designa Responsabile del Trattamento.

Il professionista, in qualità di responsabile ai sensi dell'art. 28 del Regolamento UE 2016/679, ha il potere ed il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto della normativa vigente in materia di sicurezza e tutela dei dati personali degli interessati.

Specificatamente, il responsabile è tenuto a:

- dare prova di mettere in atto opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio;
- osservare le misure organizzative e tecniche di volta in volta indicate dalla ASST Ovest Milanese;
- assistere la scrivente ASST Ovest Milanese nella valutazione dell'impatto di trattamenti di dati personali, qualora interpellato;
- assistere la scrivente ASST Ovest Milanese in caso sia necessario procedere alla consultazione preventiva dell'autorità di controllo di fronte alla presenza alti rischi, rilevati nella valutazione d'impatto;
- in presenza di collaboratori, individuare e nominare per iscritto eventuali incaricati del trattamento impartendo loro idonee istruzioni;
- vigilare sul rispetto di dette misure di sicurezza da parte dei nominati incaricati;
- dove necessario, garantire che le persone autorizzate (incaricati) si siano impegnate alla riservatezza;
- attuare gli obblighi di informazione degli interessati e acquisizione del consenso, qualora richiesto, utilizzando moduli a tal fine predisposti;
- garantire agli interessati che ne facciano richiesta l'effettivo esercizio dei diritti nei limiti e alle condizioni stabilite dalla normativa vigente;
- assicurare l'evasione tempestiva di tutte le richieste e gli eventuali reclami degli interessati;
- assicurare l'evasione tempestiva delle richieste di informazione da parte dell'Autorità Garante e dare immediata esecuzione alle indicazioni che perverranno dalla medesima Autorità;
- collaborare con i soggetti incaricati di eventuali verifiche, controlli o ispezioni;
- identificare gli eventuali nuovi trattamenti da intraprendere nella ASST Ovest Milanese, provvedendo alle necessarie formalità previste per legge;
- segnalare alla ASST Ovest Milanese qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali;

- segnalare alla ASST Ovest Milanese se un'istruzione viola le disposizioni del Regolamento o altre disposizioni previste dalla normativa cogente in materia di sicurezza e tutela dei dati personali;
- segnalare, senza ritardo, alla ASST Ovest Milanese eventuali violazioni;
- non affidare a terzi l'attività assegnata o comunque non ricorrere ad un altro responsabile senza previa autorizzazione scritta, della scrivente ASST Ovest Milanese, in qualità di Titolare del Trattamento;
- quando ricorre a un altro responsabile del trattamento, assicurare, anche mediante controllo periodico il rispetto della disciplina sulla privacy;
- mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da altro soggetto incaricato;
- al termine del proprio incarico, restituire e, se richiesto, cancellare tutti i dati personali acquisiti nell'ambito della propria funzione di responsabile del trattamento, salvo che la legislazione europea o degli Stati membri non ne preveda la conservazione.

Il professionista si impegna a mantenere indenne la ASST Ovest Milanese, da ogni danno, costo od onere di qualsiasi genere e natura, nonché da ogni contestazione, azione o pretesa avanzate nei confronti del Titolare da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità derivanti da eventuali inadempimenti del presente atto da parte del Responsabile stesso (o di eventuali suoi Sub-responsabili) o inosservanze delle istruzioni di cui al presente atto o di ulteriori istruzioni eventualmente trasmesse in modo del tutto autonomo per iscritto dal professionista.

La presente designazione decorre dalla data in cui viene sottoscritta dalle Parti ed è valida fino alla cessazione per qualunque motivo del rapporto di lavoro e/o, comunque, dei servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del rapporto di lavoro o dei servizi o alla revoca, il Responsabile dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del rapporto di lavoro.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei dati personali.

Data_____

Il Delegato dal Titolare al trattamento dei dati

_____

Data _____

Firma per ricevuta e accettazione del Responsabile del Trattamento

_____