ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO EX ART. 28 GDPR PER APPALTI/CONVENZIONI CHE IMPLICANO IMPATTI RILEVANTI AL TRATTAMENTO DEI DATI PERSONALI

La **Azienda Socio Sanitaria Territoriale (ASST) della Valtellina e dell'Alto Lario, con sede legale in Via Stelvio n. 25, Sondrio**, quale Titolare del trattamento dei dati personali e/o particolari, ai sensi dell'art. 28 del Regolamento UE/2016/679

PREMESSO CHE

- attraverso _____[1] l'ASST della Valtellina e dell'Alto Lario ha conferito a _____[2]

  nella persona del legale rappresentante _____[3] il compito di

  _____[4];

- lo svolgimento delle attività/dei servizi sopra descritte/i comporta il trattamento di dati personali nella titolarità dell'ASST della Valtellina e dell'Alto Lario;
- [inserire il nome del Responsabile] assicura che nello svolgimento di tali attività/servizi adotta tutte le misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato (art. 28 par. 1);

NOMINA

_____[5]

nella persona del legale rappresentante _____[6]

con sede legale in _____,

quale

RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dall'art. 28 par. 3 del Regolamento UE n. 679/2016 (di seguito, anche, "GDPR").

[1] Richiamare eventuali L.R. / D.G.R. / determine / convenzioni / contratti che regolamentano la fattispecie e i rapporti tra Responsabile e ASST.
[2] Inserire la denominazione / ragione sociale della società.
[3] Inserire il nome del legale rappresentante della società.
[4] Specificare l'oggetto del rapporto in essere tra le parti.
[5] Inserire la denominazione / ragione sociale della società.
[6] Inserire il nome del legale rappresentante della società.

Ambito di applicazione

Il Responsabile del trattamento esegue le operazioni di trattamento dei dati personali ad esso delegate in accordo alle istruzioni, generali e specifiche, fornite dal Titolare.

Le tipologie di dati personali di cui l'Azienda è Titolare e che sono sottoposte al trattamento da parte del Responsabile, le modalità e finalità del trattamento, nonché le categorie di persone interessate sono di seguito specificamente individuate:

Tabella - Elementi essenziali del trattamento

Tipologie di dati personali, come definiti all'art. 4 par. 1 del GDPR, oggetto del trattamento	Dati personali comuni (nome, cognome, dati di contatto, indirizzi, ecc.). Dati economici e finanziari Dati relativi allo stato di salute/Dati biometrici Dati politici/Dati Religiosi Dati relativi alla vita sessuale o all'orientamento sessuale dell'Interessato Dati giudiziari Dati genetici Altro…
Categorie di Interessati	Utenti/Pazienti Familiari dei pazienti Dipendenti Fornitori Altro…
Finalità del trattamento	Erogazione del servizio oggetto del contratto a cui la presente nomina afferisce.
Modalità del trattamento	Attraverso mezzi cartacei Attraverso mezzi elettronici

Il trattamento dei dati ha luogo anche nel territorio di uno o più Stati non appartenenti all'Unione Europea o aderenti all'Accordo sullo Spazio Economico Europeo (SEE):

☐ Si; ☐ No;

Il trasferimento extra SEE interessa i seguenti Stati:

1. _____;
2. _____;
3. _____;

In caso di trasferimento di dati verso un Paese terzo o una organizzazione internazionale, fatte salve le ipotesi in cui il Responsabile debba adempiere ad un obbligo imposto dal diritto UE o dal diritto nazionale, esso dovrà richiedere espressa e specifica autorizzazione al Titolare del trattamento e garantire che il trasferimento avvenga in sussistenza di almeno una delle condizioni di legittimità previste dal GDPR.

Autorizzazione alla nomina di sub responsabili

Con la presente nomina si fornisce espressa autorizzazione scritta generale all'individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub responsabili".

Il Responsabile del trattamento è tenuto a nominare per iscritto i sub-responsabili di cui si avvale e a comunicare al Titolare l'elenco di tutti i soggetti individuati.
Il Titolare del trattamento si riserva il diritto di verificare i nominativi dei sub-responsabili e chiederne la modifica qualora i soggetti designati non appaiano in grado di garantire il rispetto della normativa vigente e degli obblighi assunti dal Responsabile.
Il Responsabile si impegna a selezionare esclusivamente sub-responsabili che offrano garanzie sufficienti ai fini della piena conformità normativa, a verificare il rispetto delle prescrizioni in oggetto ed a fornire al Titolare evidenza delle verifiche condotte, su richiesta.
Il Responsabile si impegna a trasmettere ai sub-responsabili individuati i medesimi obblighi da esso assunti nei confronti del Titolare, con particolare attenzione al diritto di ispezione e verifica.
In ogni caso, si precisa che il Responsabile conserva nei confronti del Titolare del trattamento ogni responsabilità per l'eventuale inadempimento da parte del sub-responsabile.

Prescrizioni a carico del Responsabile del trattamento
Per lo svolgimento delle attività di trattamento connesse al servizio/all'attività di cui in Premessa, il Responsabile del trattamento dovrà attenersi alle istruzioni fornite dal Titolare.
Tutte le istruzioni saranno documentate, le istruzioni trasmesse verbalmente o telefonicamente saranno oggetto di formalizzazione non appena possibile.

Qualora una o più delle istruzioni fornite sia, a parere del Responsabile del trattamento, in contrasto con il diritto vigente, gli accordi tra le parti e le istruzioni precedenti il Responsabile dovrà immediatamente informare il Titolare.

Nello svolgimento delle attività di trattamento oggetto del presente Atto di nomina, il Responsabile dovrà:

Sicurezza del trattamento

a) adottare tutte le misure tecniche e organizzative idonee a garantire la sicurezza del trattamento con particolare riferimento allo specifico rischio connesso alla tipologia di dati trattati, così come previsto dall'art. 32 GDPR.
   Nello specifico, il Responsabile del trattamento deve:
   - ove possibile e proporzionale al trattamento eseguito, adottare tecniche di pseudonimizzazione o cifratura dei dati personali;
   - garantire su base permanente la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento;
   - garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   - garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

   In particolare, il Responsabile si impegna ad adottare – prima dell'avvio del trattamento ad esso delegato dal Titolare – le misure di sicurezza, tecniche ed organizzative, dettagliate nell'Allegato 2 del presente atto di nomina.
   Il Responsabile si impegna inoltre a mantenere le suddette misure in vigore per tutto il tempo del trattamento e di aggiornarne il contenuto, ove il trattamento richieda misure più stringenti o renda applicabili misure alternative, purché idonee a garantire un livello di sicurezza adeguato agli standard dei cui all'art. 32 GDPR.
   Il Responsabile si impegna ad avvisare il Titolare di ogni modifica apportata alle misure adottate.

Riservatezza del trattamento

b) garantire che tutte le persone incaricate del trattamento dei dati di cui l'Azienda è Titolare siano state debitamente istruite e formate, nonché che siano state vincolate alla riservatezza con riferimento ai dati in oggetto, in forma scritta o tramite un adeguato obbligo legale di riservatezza;

Collaborazione con il Titolare – Diritti degli Interessati

c) fornire la propria collaborazione, con misure tecniche ed organizzative adeguate, a favore del Titolare del trattamento affinché questi possa dare seguito alle richieste per l'esercizio dei diritti da parte dell'interessato di cui al capo III del GDPR;

d) nel caso in cui l'Interessato si rivolga direttamente al Responsabile, inoltrare immediatamente la richiesta al Titolare;

e) garantire la disponibilità dei dati trattati in formato strutturato ed accessibile;

f) trasmettere, rettificare, bloccare o cancellare immediatamente i dati trattati sotto la responsabilità del Titolare su istruzione di quest'ultimo;

Collaborazione con il Titolare – Data breach

g) assistere il Titolare del trattamento nel garantire l'adempimento degli obblighi connessi sanciti dagli artt. da 32 a 36 GDPR;

h) informare il Titolare entro 36 ore di ogni violazione, anche potenziale, dei dati personali trattati per suo conto, specificando la natura della violazione, le categorie ed il numero di dati ed interessati coinvolti (da intendersi come tale la 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 personali trasmessi, conservati o comunque trattati);

i) adottare tempestivamente tutte le misure idonee e necessarie a porre rimedio alla violazione o limitare i danni dalla stessa prodotti per gli Interessati;

Collaborazione con il Titolare – Rapporti con l'Autorità

j) supportare il Titolare nella gestione dei rapporti con l'Autorità, attraverso immediato invio delle informazioni richieste e dei documenti relativi alle misure adottate;

Collaborazione con il Titolare – DPIA

k) supportare il Titolare nell'esecuzione dell'eventuale valutazione d'impatto sulla protezione dei dati personali con riferimento ai trattamenti che coinvolgono anche il Responsabile;

l) supportare il Titolare nell'eventuale fase di consultazione dell'autorità di controllo per i trattamenti a rischio elevato in cui è previsto un suo coinvolgimento;

Conservazione

m) cancellare o restituire al Titolare del trattamento i dati personali trattati una volta conclusa la prestazione del servizio sulla base delle indicazioni e delle scelte comunicate dal Titolare del trattamento;

n) cancellare tutte le copie esistenti dei dati oggetto del trattamento dopo la scadenza dei tempi di conservazione definiti, a meno che il diritto UE o il diritto nazionale ne preveda la conservazione ulteriore;

Compliance

o) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi sanciti dal GDPR contribuendo anche alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento;

p) mettere a disposizione del Titolare l'estratto del Registro dei trattamenti ex art. 30 GDPR relativo ai trattamenti eseguiti su sua istruzione.

Inoltre, in ragione della presente nomina, si ha l'obbligo di attenersi, tra l'altro alle seguenti istruzioni:

q) vigilare attentamente affinché il trattamento che gli viene demandato sia effettuato nei termini e nei modi stabiliti dalla normativa vigente in materia di protezione dei dati personali ivi compresi i provvedimenti e le linee guida emanate dalle Autorità di controllo, le procedure adottate dal Titolare, le presenti istruzioni;

r) verificare e monitorare costantemente che il trattamento dei dati avvenga effettivamente in modo lecito e secondo correttezza nonché nel rispetto del principio di minimizzazione, assicurando che, fatti salvi eventuali obblighi di legge e/o contenzioso, i dati non siano conservati per un periodo superiore a quello necessario per gli scopi del trattamento medesimo;

s) verificare periodicamente l'esattezza e l'aggiornamento dei dati che tratta per conto del Titolare, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità per le quali sono stati raccolti o successivamente trattati.

Il Titolare si riserva, altresì, ove ne ravvisasse la necessità, di integrare ed adeguare le presenti istruzioni.

Responsabilità e diritto al risarcimento del danno.

Ai sensi e per gli effetti dell'art. 28, comma 3 del GDPR, al fine di vigilare sulla puntuale osservanza della legge applicabile e delle istruzioni impartite al Responsabile, il Titolare, anche tramite il proprio DPO e/o altro soggetto allo scopo individuato, potrà effettuare periodiche azioni di verifica.
Tali verifiche, che potranno anche comportare l'accesso a locali o macchine e programmi del Responsabile, potranno aver luogo a seguito di comunicazione da parte del Titolare, da inviare con un preavviso di almeno cinque giorni lavorativi.
Nell'ambito di tali verifiche, il Responsabile fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste del Titolare, in relazione ai dati e ai trattamenti rispetto ai quali ha valore il presente atto di nomina.

Le Parti del presente Atto sono soggette, da parte dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo all'applicazione di penali e/o alla risoluzione del rapporto principale.
Il Responsabile assume piena responsabilità diretta verso gli Interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del Titolare.
Il Responsabile si obbliga a manlevare il Titolare e tenere quest'ultimo indenne da qualsiasi tipo di conseguenza, sia civile sia amministrativa, responsabilità, perdita, onere, spesa, danno o costo da quest'ultimo sopportato che sia la conseguenza di condotte, anche omissive, imputabili al Responsabile, ovvero di violazioni agli obblighi o adempimenti prescritti dalla Normativa Privacy ovvero di

inadempimento delle pattuizioni contenute nel presente Atto di nomina, ovvero dei compiti assegnati dal Titolare.

Durata del trattamento e della nomina

Il presente Atto produce i suoi effetti a partire dalla data di sottoscrizione delle Parti e rimarrà in vigore fino alla cessazione delle attività svolte dal Responsabile a favore del Titolare, indipendentemente dalla causa di detta cessazione.

Il Trattamento, fatto salvo ogni eventuale obbligo di legge e/o contenzioso, avrà una durata non superiore a quella necessaria al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Il Legale Rappresentante di ASST della Valtellina e dell'Alto Lario

Titolare del trattamento

(Per conoscenza e accettazione)

Il Legale Rappresentante di _____ [7]

Responsabile del Trattamento

[7] Inserire la denominazione / ragione sociale della società.

Lista dei Sub-responsabili coinvolti nel trattamento

Sub-responsabile *(Nome, ragione sociale, sede legale)*	Luogo di trattamento *(Luogo in cui il trattamento è effettivamente eseguito)*	Attività delegate

Misure tecniche ed organizzative adottate dal Responsabile esterno

MISURE TECNICHE ED ORGANIZZATIVE		SI	NO	NON APPLICABILE	NOTE
1.1.	Adozione di una Politica aziendale in materia di protezione dei dati personali che garantisca e documenti la conformità a tutti i requisiti legali e normativi applicabili all'attività svolta				
1.2.	Nomina del Responsabile della protezione dei dati (DPO) / di una funzione interna deputata alla gestione degli adempimenti privacy. Nome: Numero di telefono: Indirizzo e-mail:				
1.3.	Definizione di un organigramma privacy aziendale				
1.4.	Autorizzazione al trattamento e formazione del personale che accede ai dati oggetto del trattamento.				
1.5.	Redazione del Registro dei trattamenti ex art. 30.2 GDPR.				
1.6.	Adozione di una procedura/una prassi operativa per la gestione delle richieste degli Interessati				
1.7.	Adozione di una procedura/una prassi operativa per la gestione di eventuali data breach				
1.8.	Adozione di un regolamento/una procedura/una policy sulla gestione e sull'utilizzo dei dispositivi IT				
1.9.	Implementazione di un catalogo di asset contenente la descrizione complessiva della propria architettura tecnologica				
1.10.	Adozione di misure di sicurezza ritenute adeguate in relazione alla tipologia di dati personali trattati (livello di rischio definito sulla base della tipologia di dati, categorie di interessati, numerosità degli interessati)				
Trattamento attraverso mezzi cartacei		**SI**	**NO**	**NON APPLICABILE**	**NOTE**
2.1.	Il personale incaricato al trattamento dal Responsabile è obbligato a non lasciare mai incustoditi e accessibili i documenti contenenti i dati personali trattati per conto del Titolare durante e dopo l'orario di lavoro				
2.2.	Sono individuati profili di autorizzazione differenziati per ciascun incaricato e/o per classi omogenee di incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento di competenza di ciascuno				
2.3.	Sono chiaramente identificati e comunicati agli incaricati gli archivi in cui riporre i documenti contenenti i dati personali (armadi, stanze, casseforti, ecc.).				
2.4.	La conservazione dei documenti contenenti dati personali di categorie particolari e dati giudiziari trattati sotto la titolarità dell'ASST avviene in luoghi separati e distinti da quelli di archiviazione dei documenti contenenti dati personali comuni.				
Trattamento attraverso mezzi informatici		**SI**	**NO**	**NON APPLICABILE**	**NOTE**
3.1.	Sono presenti password personali/username/misure di				

	protezione all'accesso dei sistemi con cui sono trattati i dati personali di cui l'ASST è Titolare.				
3.2.	Adozione di una procedura di autorizzazione che regoli in maniera differenziata l'accesso degli Incaricati ai dati personali di cui l'ASST è Titolare.				
3.3.	Adozione di meccanismi idonei ad evitare l'uso di password deboli da parte degli utenti.				
3.4.	Adozione di un meccanismo idoneo ad escludere l'assegnazione di un'utenza ad un incaricato diverso da quello originario.				
3.5.	Adozione di una procedura atta a garantire la sospensione delle utenze non utilizzate per oltre sei mesi.				
3.6.	Adozione di una procedura atta a garantire la pronta cancellazione delle utenze relative ad incaricati che hanno cambiato o lasciato la propria mansione.				
3.7.	Per l'amministrazione dei sistemi attivazione di un account ADMIN indipendente che differisce dall'account utente individuale ed effettivo dell'amministratore di sistema.				
3.8.	Previsione di un limite di tentativi di accesso con un nome utente / password in caso di errore.				
3.9.	Previsione di un blocco automatico dello schermo protetto da password.				
3.10.	Verifica periodica della validità delle autorizzazioni di accesso.				
3.11.	Posizionamento della sala in cui è ubicato il server/data center in luoghi adeguatamente protetti.				
3.12.	Adozione di misure di protezione dei sistemi IT dalla perdita dei dati/dall'accesso ai dati non autorizzato (es. virus, firewall, ecc.).				
Conservazione		**SI**	**NO**	**NON APPLICABILE**	**NOTE**
4.1.	Adozione di una politica formale e automatica per l'esecuzione almeno giornaliera di backup.				
4.2.	Duplicazione dei dati di backup in sedi separate e distanti almeno 10 km in linea d'aria.				
4.3.	Controlli regolari della funzionalità del ripristino da backup è controllata regolarmente.				
4.4.	Adeguate procedure di smaltimento dei supporti dati non più necessari (chiavette USB, dischi fissi) su cui sono memorizzati i dati personali di cui l'ASST è Titolare.				
Pseudonimizzazione e Cifratura		**SI**	**NO**	**NON APPLICABILE**	**NOTE**
5.1.	I dati personali sono trattati in modo pseudonimizzato/criptato. Indicazione delle tecniche ammesse:				

Luogo_____ data_____

Il Legale Rappresentante di _____ [7]

Responsabile del Trattamento