L'Azienda Socio Sanitaria Territoriale Bergamo Ovest, in qualità Titolare del trattamento dei dati personali attribuisce il ruolo di Responsabile esterno e Amministratore di sistema a……. per le seguenti attività:

…….

Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 dell'articolo 28 Regolamento 679/2016/UE e dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 e succ. modifiche. Con il termine Responsabile, d'ora in avanti, si intenderà sia il Responsabile ai sensi dell'art. 28 del Regolamento che l'Amministratore di Sistema nominato ai sensi del Provvedimento.

La presente nomina sarà oggetto di revisione/integrazione sulla base della specifica attività di auditing programmata dal Data Protection Officer (laddove nominato) individuato dal Titolare del trattamento, attività in base alla quale verranno approfonditi e sviluppati gli ambiti inerenti le specifiche misure di sicurezza adottate dal Responsabile.

Garanzie generali di sicurezza prestate dal Responsabile (Art. 28.1)

Il Responsabile del trattamento (d'ora in avanti "Responsabile") garantisce l'attuazione di misure tecniche ed organizzative tali da soddisfare, nella loro totalità, i requisiti posti dal Regolamento.

Autorizzazione nomina Sub-Responsabili (Art. 28.2 – 28.4)

Ai sensi dell'art.28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub-responsabili". A fronte di tale autorizzazione, si richiede al Responsabile di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di sub-responsabili. La scrivente provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile del trattamento individuare e nominare in forma scritta i propri sub-responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del sub-responsabile i medesimi obblighi posti a carico del responsabile e specificati nel presente documento, in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenza come il Responsabile conservi nei confronti della scrivente, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal sub-responsabile.

Prescrizioni poste a carico del Responsabile (art. 28.3)

Per lo svolgimento delle attività di trattamento dati personali conseguenti al servizio affidato al Responsabile, lo stesso dovrà:

a. comunicare preventivamente l'eventuale trasmissione dei dati personali verso paese terzo (non appartenente alla Unione Europea); in tali casistiche il Titolare si riserva la facoltà di esprimere apposita autorizzazione alla trasmissione a meno che tale trasmissione non sia espressamente richiesta dell'Unione o dal diritto nazionale;

b. autorizzare espressamente al trattamento dei dati personali i propri dipendenti/collaboratori/soci/volontari attraverso modalità che garantiscano che tali soggetti siano obbligati al rispetto della riservatezza nei confronti dei dati che si troveranno a trattare in funzione del proprio incarico/ruolo;
c. garantire di aver effettuato una analisi dei rischi sui trattamenti oggetto della responsabilità e assistere il Titolare del trattamento nella valutazione di impatto ai sensi dell'art. 35 del Regolamento tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; i documenti comprovanti l'analisi del rischio dovranno essere messi a disposizione del Titolare del trattamento su richiesta di quest'ultimo;
d. garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al titolare nel caso di esplicita richiesta;
e. garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al titolare nel caso di esplicita richiesta;
f. 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; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al titolare nel caso di esplicita richiesta;
g. garantire che tutti i soggetti che agiscono sotto l'autorità del responsabile e che abbiano accesso ai dati non trattino tali dati se non sono stati istruiti in tal senso dal Responsabile stesso;
h. garantire il necessario apporto al titolare del trattamento qualora nei confronti di questo vengano esercitati i diritti che il Regolamento (al capo III) riconosce agli interessati i quali impattino sui dati personali oggetto della presente nomina;
i. garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del regolamento. La comunicazione da parte del responsabile al titolare dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC istituzionale e dovrà contenere almeno i seguenti punti:
    a. natura della violazione 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;
    b. il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
    c. descrivere le probabili conseguenze della violazione dei dati personali;
    d. descrivere le misure adottate da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

    Il responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite.

j. cancellare e/o restituire al titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione;
k. rendersi disponibile a sottoporsi ad attività di auditing da parte del titolare del trattamento, o di un delegato di quest'ultimo, qualora questo ne ravvisasse la necessità;
l. comunicare al titolare del trattamento l'adesione ad eventuali codici di condotta di cui all'articolo 40 o ad un meccanismo di certificazione di cui all'articolo 42 del Regolamento;
m. attenersi ai criteri di durata del trattamento comunicati dal Titolare.

Prescrizioni poste a carico del Responsabile ai sensi del Provvedimento a carattere generale sugli Amministratori di Sistema dell'Autorità Garante Privacy del 27 Novembre 2008

Ai sensi del Provvedimento il Responsabile è stato individuato dal Titolare del trattamento dei dati personali in base ad una scrupolosa valutazione dell'esperienza, della capacità, dell'affidabilità e preparazione e fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

Il Responsabile ha quindi, il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle vigenti disposizioni in materia di trattamento dei dati personali ivi compreso il profilo relativo alla sicurezza.

Il Responsabile garantirà al Titolare del trattamento che ciascun incaricato Amministratore di Sistema accederà con proprio utente e propria password.

Con l'accettazione di questa nomina il Responsabile si impegna a nominare individualmente - ai sensi del Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 (G.U. N. 300 Del 24 dicembre 2008) cosi come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25 giugno 2009 (G.U. N. 149 Del 30 giugno 2009) - gli incaricati della sua struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Annualmente il Responsabile fornirà al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema e provvederà a verificare l'attività dei soggetti individuati, come indicato dal Garante Privacy nel Provvedimento sugli Amministratori di Sistema sopra richiamato.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il Responsabile è tenuto a:

- garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto a seguito di apposita comunicazione in tal senso del Titolare del trattamento, utilizzando gli opportuni meccanismi di identificazione e autenticazione allo scopo di incrementare il livello di protezione e sicurezza dei trattamenti di dati personali effettuati con strumenti elettronici;
- essere responsabile della gestione dei sistemi di identificazione ed autenticazione, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge, eseguendo controlli periodici sull'efficacia delle misure di sicurezza adottate;
- collaborare con il Titolare del trattamento dei dati alla definizione di idonee regole in ambito di Sicurezza del trattamento dei dati afferente ai sistemi oggetto della presente nomina;
- sovrintendere all'operato dei soggetti terzi idoneamente designati, qualora sia necessario, interni o esterni al Titolare, in caso di interventi tecnici che abbiano impatto sul sistema informativo del Titolare e sulla sicurezza del trattamento di dati;
- suggerire, curare e sovraintendere l'adozione e l'aggiornamento delle più ampie misure di sicurezza volte a far sì che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- aggiornare periodicamente, con frequenza adeguata, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti o assicurarsi che ciò venga effettuato da soggetti terzi idoneamente designati;

- coadiuvare il Titolare del trattamento ed i Responsabili interni ed esterni, eventualmente designati, nell'attuazione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- svolgere un ruolo di primaria interfaccia nella scelta delle dotazioni informatiche, nessuna esclusa, quali hardware di qualsiasi genere, software e qualsiasi altro dispositivo elettronico, e di tutti i processi tecnologici del Titolare, coadiuvando le singole unità organizzative nel processo decisionale sulle suddette dotazioni informatiche;
- svolgere un ruolo di primaria interfaccia, coadiuvando i Responsabili interni ed esterni della struttura informatica, nel caso di incidenti/malfunzionamenti di qualsiasi genere che riguardino la rete, le attrezzature informatiche e l'utenza, e preoccuparsi di erogare una corretta informazione verso gli utenti; dovrà inoltre supportare il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo;
- svolgere un ruolo di primaria interfaccia coadiuvando i Responsabili delle unità organizzative nell'innovazione della struttura IT, proseguendo l'innovazione tecnologica al fine di dotare il Titolare di un moderno Sistema di gestione informatica, ottimizzandone i processi;
- sovrintendere alle operazioni di coordinamento e funzionamento della rete informatica interna;
- eseguire direttamente o assicurarsi che venga fatto da soggetti terzi idoneamente designati le copie di sicurezza e ripristino, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge.

Responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi posti dal Regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare nel presente atto.

In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento.

In caso di accertata violazione delle disposizioni del Regolamento o del presente contratto, il Titolare si riserva il diritto di mettere in atto le misure ritenute corrette nei confronti del Responsabile. Se la violazione si configurasse di particolare gravità, è fatto salvo il diritto del Titolare di rescindere il presente contratto.

Durata e risoluzione

Le prescrizioni di cui al presente atto hanno decorrenza dall'ultima data di sottoscrizione e scadenza congrua a quella indicata nel rispettivo contratto di fornitura di servizi. Il presente atto rimarrà in vigore fino a quando continueranno a svilupparsi le obbligazioni contrattuali del contratto di fornitura dei servizi di cui l'atto stesso disciplina gli aspetti inerenti la tutela dei dati personali.

Luogo e data _____

Per conto del Titolare del Trattamento	**Firma per accettazione del Responsabile**
	.....