AZIENDA SANITARIA PROVINCIALE
di PALERMO

Prot. n._____ del_____

NOMINA A SOGGETTO AUTORIZZATO

Oggetto: ***Nomina "Persone autorizzate al trattamento" di dati personali ai sensi degli artt. 28 paragrafo 3, lett. b), 29 e 32 paragrafo 4 del Regolamento UE 2016/679 (GDPR) e dell'art. 2-quaterdecies del D.Lgs. 196/2003 così come integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.***

Visto il 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 (di seguito indicato "**GDPR**"), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali.

Visto il D.Lgs. 30 Giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (di seguito "**Codice Privacy e ss.mm.ii.**")

Considerato che lo svolgimento delle attività Istituzionali dell'Azienda Sanitaria Provinciale di Palermo comporta il trattamento di dati personali e dati personali particolari che sono tutelati dal GDPR, dal Codice Privacy e ss.mm.ii. nonché dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali (di seguito "**Normativa Privacy Applicabile")**

Considerato che, ai fini del GDPR per:

- *"trattamento"* si intende ai sensi dell'art. 4 del GDPR, *"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"*
- *"Dato personale"* si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. art. 4.1, GDPR);
- "*categorie particolari di dati personali*" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, comma 1, GDPR);
- "*dati personali relativi a condanne penali e reati*" si intendono i dati personali di cui all'art. 10 del GDPR.

Preso atto che l'art. 29 del GDPR stabilisce la regola generale per cui "*chiunque agisca sotto l'autorità del Responsabile del Trattamento o sotto quella del Titolare del Trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

Preso atto che l'art. 2-*quaterdecies* del Codice Privacy e ss.mm.ii. prevede esplicitamente che "*il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.*";

Preso atto che, alla luce dell'art. 30 del GDPR, l'Azienda Sanitaria Provinciale di Palermo ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante per ciascuna Unità Operativa le informazioni in ordine ai trattamenti effettuati dall'Azienda Sanitaria Provinciale di Palermo;

Preso atto che è stato designato il Responsabile della Protezione dei Dati Personali (RPD) del l'Azienda Sanitaria Provinciale di Palermo - in conformità a quanto prescritto dall'art. 37 del GDPR;

Ciò premesso,

il sottoscritto Dott. _____ RESPONSABILE DELL'UNITA' OPERATIVA _____, nominato dal Direttore Generale dell'Azienda Sanitaria Provinciale di Palermo, in qualità di Titolare del Trattamento, quale Delegato al trattamento, in conformità a quanto prescritto ai sensi dell'art. 2 – quaterdecies del D.lgs. 196/2003 e ss.mm.ii., nomina la S.V. _____ **,**

PERSONA AUTORIZZATA AL TRATTAMENTO

relativamente alle attività aziendali svolte nell'Unità Operativa, in conformità e nei limiti delle proprie competenze espresse in ordini di servizio e circolari dell'Azienda Sanitaria Provinciale di Palermo, in particolare:

- (indicare i trattamenti effettuati) _____
- (indicare i trattamenti effettuati) _____

I trattamenti effettuati dalla suddetta Unità Operativa sono quelli riportati nel "Registro delle attività di trattamento" predisposto dall'Azienda Sanitaria Provinciale di Palermo ai sensi dell'art. 30 del GDPR e disponibile per la consultazione presso la sede del Titolare.

In questo ambito l'autorizzato dovrà rispettare le seguenti disposizioni:

- nel trattare i dati personali deve operare garantendo la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati personali confidenziali e, di norma, soggetti ad un dovere di riservatezza. Pertanto, non si dovranno divulgare a terzi le informazioni di cui si è venuti a conoscenza;
- trattare i dati in modo lecito e secondo correttezza;
- adottare tutte le misure necessarie a verificare l'esattezza dei dati raccolti e registrati, e se necessario, correggerli ed aggiornarli di conseguenza;
- comunicare tempestivamente e senza ingiustificato ritardo al Delegato e/o in assenza direttamente al Titolare ed al RPD le eventuali violazioni dei dati o gli incidenti informatici (data breach) che possono avere un impatto significativo sui dati personali, al fine di consentire all'Azienda Sanitaria Provinciale di Palermo di comunicare al Garante Privacy, entro settantadue (72) ore dalla conoscenza del fatto, tali eventi secondo quanto previsto nel GDPR e comunque nel rispetto delle policy dell'Azienda Sanitaria Provinciale di Palermo sugli incidenti relativi alla sicurezza delle informazioni e alla violazione dei dati personali;
- mettere in atto tutti gli accorgimenti necessari per assicurare la riservatezza, l'integrità e la disponibilità dei dati trattati nel rispetto delle disposizioni impartite dall'Azienda Sanitaria Provinciale di Palermo;

- adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso della persona Autorizzata; in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'Autorizzato dovrà verificare che non vi sia possibilità, da parte di terzi, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, sia cartaceo che informatizzato.
  In particolare, per chiunque abbia accesso a sistemi/applicazioni dell'Azienda Sanitaria Provinciale di Palermo, dovranno essere osservate le seguenti disposizioni:
  - le viene fornito, dalla Direzione ICT, un codice di identificazione (username), che dovrà provvedere a mantenere segreto. Qualora avesse il sospetto che terzi siano venuti a conoscenza dello stesso, dovrà informare immediatamente il Delegato al trattamento di riferimento;
  - le viene fornita una parola chiave (password), composta da otto caratteri alfanumerici che dovrà provvedere a modificare in occasione del primo accesso, e successivamente almeno ogni sei mesi, nel caso in cui lei tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui Lei tratti anche dati particolari e dati relativi alla salute. Le raccomandiamo di fare uso di caratteri alfanumerici, che formano un codice non banale e che non abbia alcun riferimento con i propri dati personali (nomi, indirizzi, date di nascita…) Suoi, di suoi parenti, amici, colleghi o comunque conoscenti;
  - la parola chiave deve essere da Lei mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia;
- svolgere le sole operazioni di trattamento consentite e conformi ai fini istituzionali per i quali i dati sono stati raccolti e trattati;
- collaborare con il Delegato per l'aggiornamento del "Registro delle attività di trattamento", di cui all'art. 30 del GDPR, e afferenti l'unità Operativa di appartenenza, laddove richiesto dal medesimo;
- comunicare tempestivamente, qualora necessario, al Delegato o al RPD dell'Azienda Sanitaria Provinciale di Palermo, ogni circostanza idonea a determinare un pericolo di dispersione o utilizzazione non autorizzata dei dati stessi nonché ogni evento legato a operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle definite dall'Azienda Sanitaria Provinciale di Palermo;
- le raccomandiamo di non disattivare i software di protezione di cui dispone la nostra organizzazione, le cui specifiche tecniche Le verranno fornite, oltre che in questa sede, ogni volta che vi sono dei significativi aggiornamenti. Sottolineiamo, in particolare, l'importanza di non aprire file di provenienza non certa o sospetta e di adottare diligentemente le opportune cautele, al momento della trasmissione all'esterno di nostri files (es. file in formato .zip protetto da password);
- per lo svolgimento delle Sue mansioni lavorative, Le verrà attribuita, se necessario, una casella di posta elettronica aziendale. Le raccomandiamo di utilizzarla esclusivamente per finalità legate alla Sua attività lavorativa ovvero secondo quanto previsto dalle "Norme comportamentali per il corretto utilizzo dei sistemi informatici e dei telefoni e fax aziendali" (Prot. 2207/URP – 18 nov. 2008);
- le verrà attribuito, se necessario, l'accesso ad Internet, del quale La invitiamo ad usufruire solo nei limiti necessari per lo svolgimento dell'attività lavorativa ovvero secondo quanto previsto dalle "Norme comportamentali per il corretto utilizzo dei sistemi informatici e dei telefoni e fax aziendali" (Prot. 2207/URP – 18 nov. 2008);
- le ricordiamo che è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore;
- prima di procedere al download di software, anche a titolo gratuito, non espressamente autorizzato dall'Azienda, dovrà inoltre chiedere l'autorizzazione al proprio Delegato del trattamento e Servizio Informatico Aziendale;
- per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati personali, può rivolgersi al Delegato al trattamento di riferimento per ricevere le opportune istruzioni.

Per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Delegato o dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati, avendo particolare riguardo a:

- i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
- atti e documenti contenenti dati particolari o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione;
- atti e documenti contenenti dati particolari o giudiziari devono essere restituiti al termine delle operazioni affidate;
- eventuali fotocopie o copie di documenti devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

Ulteriori istruzioni rispetto a quelle elencate Le potranno, di volta in volta, essere fornite dal Titolare e/o dal Delegato al Trattamento, in base alla normativa applicabile.

La presente Autorizzazione è determinata ai sensi della normativa applicabile in materia di protezione dei dati personali, in considerazione delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare.
Pertanto, resta inteso che la presente nomina avrà la medesima durata del suo rapporto con l'Azienda Sanitaria Provinciale di Palermo e che, successivamente alla cessazione dello stesso, Lei non sarà più autorizzato/a ad effettuare alcun tipo di trattamento sui dati e sarà, comunque, tenuto/a ad osservare il massimo riserbo su qualsiasi informazione o circostanza di cui fosse venuto/a a conoscenza nel corso del suo percorso lavorativo presso l'Azienda Sanitaria Provinciale di Palermo
Nel firmare la presente nomina, Lei si impegna formalmente all'obbligo legale di riservatezza dei trattamenti effettuati così come richiesto dal GDPR. Inoltre, si rende consapevole che l'inadempimento dell'obbligo di diligente e corretta esecuzione delle istruzioni ricevute in ordine a quanto sopra, ed in particolare la violazione del divieto di comunicazione e diffusione dei dati trattati, come sopra specificato, potrà costituire elemento di valutazione dell'attività svolta per conto dell'Azienda Sanitaria Provinciale di Palermo, Titolare del Trattamento dei Dati.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Distinti saluti,

data _____

_____
Il Delegato al trattamento
Unità Operativa _____
(nome e cognome Delegato al trattamento):_____

Per presa visione dell'autorizzazione ricevuta e accertamento della consapevolezza delle informazioni ricevute.

_____ _____
(Nome e Cognome) (firma)

Oggetto "Nomina a Responsabile del trattamento dei dati personali ai sensi degli artt. 4.8 e 28 del GDPR – Regolamento (UE) 679/2016 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".

Prot. n. _____/ Palermo lì_____

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
Allegato al CONTRATTO N°..... DEL ...../..... /....., relativo alla DELIBERA N° ..... DEL ..../..../.....

TRA

L'Azienda Sanitaria Provinciale di Palermo con sede legale in via Giacomo Cusmano n.24 90141 Palermo, C.F. e P.I.V.A. n. 05841760829, nella persona del legale rappresentante pro tempore Dott.ssa Daniela Faraoni nonché in qualità di Commissario Straordinario;

E

La **<*indicare ragione e denominazione sociale della Società*>** **(**di seguito, per brevità, anche Società) con sede in ……in persona del legale rappresentante pro tempore Dott. ……;

PREMESSO CHE

L'Azienda Sanitaria Provinciale di Palermo, in qualità di **TITOLARE DEL TRATTAMENTO DI DATI PERSONALI,** svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi istituzionalmente affidati;

L'Azienda Sanitaria Provinciale di Palermo, in qualità di Titolare del trattamento è consapevole di essere tenuto a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e di essere tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

VISTO che il 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 (di seguito GDPR), garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;

VISTO il D. Lgs. 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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"* come novellato dal D. Lgs. 10 agosto 2018, n. 101 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE"*;

PRESO ATTO che l'art. 4.2 del GDPR definisce «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;

PRESO ATTO che l'art. 4.7 del GDPR definisce "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;

PRESO ATTO che l'art. 4.8 del GDPR definisce "Responsabile del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

VISTO che le attività, erogate in esecuzione del Contratto **n°..... del ...../...../..... relativo alla Delibera n° ..... del ...../...../.....** in essere tra l'Azienda Sanitaria Provinciale di Palermo e ***<indicare ragione e denominazione sociale della Società>,*** implicano da parte di quest'ultima, il trattamento dei dati personali di cui è Titolare il Azienda Sanitaria Provinciale di Palermo, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

VISTO che in data 24/12/2008 è stato pubblicato sulla Gazzetta Ufficiale 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", emanato in data 27/11/2008 e successivamente modificato ed integrato;

VISTO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

VISTO che le "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni",* emanate dall'AgiD in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito per brevità "*Misure minime AgID*"), hanno dettato le regole da osservare per garantire un uso appropriato dei privilegi di Amministratore;

VISTO che, ai sensi del comma 1 dell'art. 28 del GDPR, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui l'Azienda Sanitaria Provinciale di Palermo è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal GDPR;

Quanto sopra premesso, le parti stipulano e convengono quanto segue.

L'Azienda Sanitaria Provinciale di Palermo **NOMINA** ***<indicare ragione e denominazione sociale della Società>***, quale **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** in virtù del presente atto di designazione, ai sensi e per gli effetti delle vigenti disposizioni normative contenute negli artt. 4.8 e 28 del GDPR, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto dichiara di essere edotta di tutti gli obblighi che incombono sul Titolare del trattamento e si impegna a rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica, attenendosi alle disposizioni operative contenute nel presente atto e di seguito enunciate:

- I trattamenti dovranno essere svolti nel pieno rispetto delle previsioni legislative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare:
  - i trattamenti sono svolti ***<indicare le finalità per cui il fornitore tratta i dati ovvero l'oggetto del contratto>***;
  - i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto:
    - dati di natura personale (art. 4.1 GDPR);
    - dati sensibili (art. 9 del GDPR "Categorie particolari di dati personali");

- dati giudiziari (art. 10 del GDPR); ***<eliminare le eventuali tipologie di dati non oggetto di trattamento>***

- le categorie di interessati sono ***<indicare le tipologie di interessato (dipendenti/collaboratori) cui i dati afferiscono>*.**

- La Società si dichiara già in possesso di garanzie sufficienti per la messa in atto in termini di conoscenza specialistica, affidabilità e risorse, di misure tecniche ed organizzative adeguate a garantire che il trattamento dei dati soddisfi i requisiti del Regolamento UE 2016/679 nonché si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita" di cui all'art. 25 del GDPR (*privacy by design/default)*, a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, di cui all'art. 32 del GDPR, prima dell'inizio delle attività.

- La Società dovrà eseguire i trattamenti funzionali alle attività ad essa attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, la Società dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo.

- La Società dovrà garantire in ogni caso l'obbligo di riservatezza; inoltre, i dati potranno essere trattati anche al fine di assolvere ad obblighi di legge, nonché nell'ambito delle proprie procedure interne in tema di controllo di qualità e gestione del rischio, da ritenersi inscindibilmente connesse e funzionali all'erogazione della prestazione professionale. Dette procedure sono finalizzate a presidiare il rispetto degli standard di qualità e indipendenza posti del Responsabile nel primario interesse del Titolare.

- La Società dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarle nei loro compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo anche in modo che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. La Società dovrà garantire, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza nonché che ricevano la formazione necessaria in materia di protezione dei dati personali.

- In particolare, tenuto conto dello stato dell'arte e dei costi di attivazione delle misure di sicurezza adottate a protezione dei trattamenti dei dati per conto del Titolare come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:
  - la pseudonimizzazione e la cifratura dei dati personali;
  - misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
  - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- la valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

In aggiunta la Società, ove applicabile, dovrà adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID n. 2/2017 del 18 aprile 2017, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti.

- La Società dovrà predisporre e tenere a disposizione della documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal GDPR, consentendo di effettuare periodicamente attività di verifica/audit, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato. Dette verifiche dovranno essere eseguite senza pregiudizio delle normali attività, in orari da concordare e con modalità che consentano il rispetto degli obblighi di riservatezza e confidenzialità nei confronti di altri soggetti e che in ogni caso non ledano o mettano in alcun modo in pericolo i segreti aziendali del Responsabile e/o il suo know-how. In alternativa, per l'esecuzione delle predette verifiche, il Responsabile potrà avvalersi di soggetti esterni di comprovata esperienza e trasmettere la risultanza al Titolare.

- La Società inoltre riconosce all'Azienda Sanitaria Provinciale di Palermo il diritto di effettuare controlli (Audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali del Titolare. A tal fine l'Azienda Sanitaria Provinciale di Palermo potrà periodicamente sottoporre alla Società un questionario sul livello di sicurezza e conformità alla normativa in materia dei dati personali (che dovrà essere debitamente compilato e restituito) e ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di Audit o di rendicontazione in ambito di protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile .

- Anche per le finalità sopraesposte, la Società è obbligata a mettere a disposizione in qualunque momento e su richiesta del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina ed è altresì tenuto a contribuire alle attività di revisione realizzate dal Titolare del trattamento o da un altro soggetto da questo incaricato, comprese le ispezioni

- La Società, ai sensi dell'art. 30 del GDPR e nei limiti di quanto esso prescrive, è tenuta a tenere un Registro delle attività di Trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR. Inoltre, la Società si impegna a comunicare al Titolare del trattamento ogni elemento utile per la predisposizione delle informazioni di cui agli art. 13 e 14 del GDPR.

- La Società è tenuta ad informare di ogni violazione di dati personali *(cd. data breach*), tempestivamente, e in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, il Titolare ed il Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo. Tale notifica – da effettuarsi tramite PEC da inviare sia all'indirizzo PEC del Titolare ***<indicare indirizzo PEC>*** - deve essere accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR, per permettere al Titolare, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. La società, dovrà fornire tutti i dettagli completi della violazione subita; in particolare: una descrizione della natura della violazione dei dati personali, le circostanze in cui è avvenuta, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali

sull'Azienda Sanitaria Provinciale di Palermo e sugli interessati coinvolti ed i provvedimenti adottati (o che si intendono adottare) per porvi rimedio ed attenuare i possibili effetti negativi, indicando il Responsabile della Protezione dei Dati (Data Protection Officer), con i relativi dati di contatto. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, la Società supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in suo possesso e/o di suoi sub-Responsabili.

- La Società, su eventuale richiesta del Titolare, è tenuto inoltre ad assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del GDPR.

- La Società, qualora riceva istanze degli interessati in esercizio dei loro diritti di cui dall'art. 15 all'art. 22 del GDPR, è tenuta a:
  - darne tempestiva comunicazione scritta al Titolare o al Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo, allegando copia della richiesta;
  - valutare con il Titolare e con il Responsabile della Protezione dei Dati (RPD) del Azienda Sanitaria Provinciale di Palermo la legittimità delle richieste;
  - coordinarsi con il Titolare e con il Responsabile della Protezione dei Dati (RPD) del Azienda Sanitaria Provinciale di Palermo al fine di soddisfare le richieste ritenute legittime.

- La Società è autorizzata a nominare altri responsabili (di seguito, "Sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, necessarie all'esecuzione del contratto, e in tale ipotesi si impegna a rispettare le condizioni dell'art 28 del Regolamento EU2016/679 e conseguentemente a informare, a mezzo pec, il Titolare del Trattamento di eventuali modifiche previste al processo di trattamento riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

- La Società, nel caso in cui, per le prestazioni del Contratto **n°..... del ...../...../..... relativo alla Delibera n° ..... del ...../...../.....** che comportano il trattamento di dati personali, ricorra a subappaltatori o subcontraenti, è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al Titolare. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportati in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate, di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti.

- La Società deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante nel caso in cui siano inerenti il trattamento dei dati effettuato per conto del Titolare. Inoltre nel garantire gli adempimenti e le incombenze anche formali verso l'Autorità Garante quando richiesto e nei limiti dovuti, collabora tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità Garante per la protezione dei dati personali. In particolare:
  - fornisce informazioni sulle operazioni di trattamento svolte;
  - consente l'accesso alle banche dati oggetto delle operazioni di trattamento;

- consente l'effettuazione di controlli;
- compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.

- La Società si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato di cui agli artt. 40 e 42 del GDPR quando verranno emanati. Il Titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

- La Società non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare. La Società si impegna a limitare gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE, che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal GDPR (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello e etc.). Inoltre, la Società dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione, consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente Contratto.

- La Società è obbligata altresì, a comunicare immediatamente all'Azienda Sanitaria Provinciale di Palermo il verificarsi di una delle seguenti fattispecie:
  - mancato rispetto delle clausole contrattuali standard di cui sopra; oppure
  - qualsiasi modifica della metodologia e delle finalità di trasferimento dei dati personali dell'Azienda Sanitaria Provinciale di Palermo fuori dalla Comunità Europea.

- La Società è tenuta a comunicare al Titolare ed al Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo il nome ed i dati del proprio RPD, laddove la società stessa lo abbia designato conformemente a quanto prescritto dall'art. 37 del GDPR. Il RPD collaborerà e si terrà in costante contatto con il RPD dell'Azienda Sanitaria Provinciale di Palermo. A tal fine il Titolare comunica al Responsabile che il proprio "Responsabile della Protezione dei Dati" è il Dott. Giuseppe Buttafuoco designato conformemente all'art. 37 del Regolamento UE, reperibile all'indirizzo mail: rpd@asppalermo.org

- La Società, ove applicabile, è tenuta a mettere in atto tutte le misure necessarie per ottemperare al 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", emanato in data 27/11/2008 e successive modifiche ed integrazioni. Ovvero si impegna a:
  - designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
  - predisporre e conservare l'elenco contenente gli estremi identificativi delle persone qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
  - comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema;
  - verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica.

- La Società, ove applicabile, è tenuta a mettere in atto tutte le "misure minime di sicurezza ICT per le PP.AA." (livello minimo) prescritte dall'Agenzia per l'Italia Digitale (AgID) con Circolare n. 2/2017 del 18 aprile 2017.

- La Società, nel caso in cui, agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento sarà chiamata a rispondere delle inadempienze contrattuali secondo quanto stabilito nel contratto in essere tra le parti al quale la presente è allegata e parte integrante.
- Il Titolare del trattamento dichiara che tutte le comunicazioni inerenti i compiti, le funzioni e gli obblighi derivanti dal presente atto di nomina, gli potranno essere trasmesse ai seguenti riferimenti. PEC: direzionegenerale@pec.asppalermo.org o rpd@pec.asppalermo.org ; ovvero all'indirizzo della propria sede: Via Giacomo Cusmano n 24 - 90141 Palermo (PA).

  Il Responsabile del trattamento dichiara che tutte le comunicazioni inerenti i compiti, le funzioni e gli obblighi derivanti dal presente atto di nomina, gli potranno essere trasmesse ai seguenti riferimenti. PEC: ***<indicare indirizzo PEC>***.ovvero all'indirizzo della propria sede: ***<indicare indirizzo sede.>.***

La presente nomina avrà efficacia fino al termine del suindicato contratto in essere tra l'Azienda Sanitaria Provinciale di Palermo e la Società ovvero sino alla rinuncia o revoca del contratto in essere tra le parti.
All'atto della cessazione dei contratti in essere con l'Azienda Sanitaria Provinciale di Palermo, la Società, sulla base di quanto stabilito dal contratto, restituirà i dati personali oggetto del trattamento oppure provvederà alla loro integrale distruzione, salvo che i diritti dell'Unione e degli Stati membri ne prevedano la conservazione.
Tuttavia, la Società avrà facoltà di mantenere i dati trattati al solo fine di assolvere ad obblighi legali di conservazione e rispettare le proprie procedure in tema di documentazione dell'attività professionale svolta (ad esempio per richiesta di un'Autorità o in caso di contenzioso di qualsivoglia natura) salvo la conservazione della documentazione in ottemperanza delle normative vigenti quali a titolo esemplificativo quelle contabili e fiscali.

La validità del presente atto si intende altresì estesa ad ulteriori, eventuali, proroghe contrattuali; ogni altra pattuizione resta pienamente confermata e impregiudicata.

Il Titolare del Trattamento dei Dati

Azienda Sanitaria Provinciale di Palermo

(firma digitale)

Il presente atto deve essere firmato digitalmente dal Legale Rappresentante di ***<indicare Ragione sociale e riferimenti della Società>*** e inviato a mezzo PEC all'indirizzo direzionegenerale@pec.asppalermo.org e rpd@pec.asppalermo.org
Sottoscrivendo il medesimo atto, ***<indicare Ragione sociale e riferimenti della Società>***

(a) conferma di conoscere gli obblighi assunti in relazione alle disposizioni del GDPR e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal predetto decreto e sue eventuali modifiche ed integrazioni;
(b) conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;
(c) accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni decise dal Titolare, anche in ottemperanza alle evoluzioni legislative in materia.

Timbro e firma digitale del Responsabile del Trattamento
(Legale Rappresentante della Società)

_____