Servizio Sanitario Regionale Basilicata
Azienda Sanitaria Locale di Potenza

DELIBERAZIONE DEL DIRETTORE GENERALE	
NUMERO 2019/00098	**DEL** 12/02/2019

☑ Collegio Sindacale il **12/02/2019**

OGGETTO

Organizzazione e individuazione dei soggetti competenti in materia di protezione dei dati personali ai sensi del Regolamento UE 2016/679 e D.lgs n.101/2018

Struttura Proponente	Comunicazione e Relazioni Esterne - (PZ)

Documenti integranti il provvedimento:

Descrizione Allegato	Pagg.	Descrizione Allegato	Pagg.
Modulistica	9		

Uffici a cui notificare

Attività Tecniche - (PZ)	Economato - Provveditorato
Sistema Informativo Automatizzato e Tecn. dell'Informaz.	Comunicazione e Relazioni Esterne - (PZ)

CERTIFICATO DI PUBBLICAZIONE

La presente è stata pubblicata ai sensi dell'Art.32 della L.69/2009 all'Albo Pretorio on-line in data 12/02/2019

La presente diviene eseguibile ai sensi dell'art.44 della L.R. n.39/2001 e ss.mm.ii

☑ Immediatamente ☐ Dopo 5 gg dalla pubblicazione all'Albo ☐ Ad avvenuta approvazione regionale

Il Dirigente dell'UOSD Trasparenza S.A., Dott. Antonio Bavusi> relaziona quanto segue:

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 e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati - GDPR), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018;

Visto il Decreto Legislativo n. 101/2018 recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 succitato;

Richiamato in particolare l'art. 5 del GDPR, che al comma 1 enuncia i principi applicabili al trattamento dei dati personali e al comma 2 pone in capo al titolare il principio di responsabilizzazione e rendicontazione (cd. accountability), in base al quale lo stesso deve assicurare, ed essere in grado di comprovare, il rispetto di tali principi;

Viste le Delibere del Direttore Generale n. 10/2011 e 251/2011 con cui venivano nominati i Responsabili dei Trattamenti di Dati Personali ai sensi dell'art. 29 del D.Lgs. 196/2003;

Dato atto che la responsabilizzazione del titolare si realizza anche mediante:

- la concreta adozione, sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso, di misure tecniche e organizzative adeguate ed efficaci, che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche (privacy by design);

- l'adozione di misure tecniche ed organizzative adeguate che garantiscano che siano trattati soltanto i dati personali necessari per ciascuna finalità di trattamento (privacy by default);

- l'individuazione di un Responsabile della Protezione dei Dati (RPD) – obbligatorio per le Pubbliche Amministrazioni - che, tra le altre funzioni, fornisce indicazioni e vigila sulla corretta osservanza del GDPR all'interno dell'organizzazione del titolare;

Vista la Delibera Commissariale n. 537/2018 con la quale si è proceduto a nominare il RPD per l'Ente nella persona dell'ing. BRUNO Gianfranco;

Dato atto che Titolare del trattamento è la stessa Azienda Sanitaria Locale di Potenza;

Considerato che il Regolamento (UE) 2016/679, oltre ad indurre nel titolare una sostanziale revisione delle proprie politiche in materia di privacy, dovuta in particolar modo all'applicazione del succitato principio di 'accountability', ovvero responsabilizzazione e rendicontazione, innova sia il glossario sia i ruoli privacy e le responsabilità connesse all'interno dell'organizzazione del titolare e innesta all'interno della struttura organizzative nuove responsabilità sulla protezione dei dati, ritenendo che il dato, per il suo valore economico sociale ed organizzativo, sia una risorsa assegnata alla responsabilità dell'azione dirigenziale alla stregua di quelle finanziarie ed umane;

Ritenuto per quanto sopra di procedere ad un adeguamento dell'organizzazione privacy nell'Ente secondo le previsioni dell'art. 2-quatordecies del D. Lgs. 101/2018 attribuendo specifici compiti e funzioni connessi al trattamento di dati personali a persone fisiche all'uopo designate che opereranno sotto l'autorità del Titolare nell'ambito del proprio assetto organizzativo;

Ritenuto di autorizzare gli operatori (dipendenti e non) assegnati alle strutture afferenti ai soggetti designati, che agiscono sotto la loro autorità, al trattamento dei dati personali, nel rispetto del principio di minimizzazione dei dati, istruendoli sulle modalità del trattamento come riportato nell'allegato 1), parte integrante e sostanziale del presente atto, stabilendo che l'ambito di operatività di ciascun autorizzato (tipi di dati personali trattati, operazioni di trattamento eseguibili, banche dati cui accedere ecc.) verrà individuato con successivo apposito provvedimento del Direttore Generale.

Considerato che ogni soggetto che tratta dati personali per conto dell'Ente deve essere individuato responsabile dei trattamenti nei modi e nelle forme previsti all'art. 28 del GDPR;

Ritenuto inoltre di individuare come Amministratori di sistema (AdS - Provvedimenti del Garante del 27/11/2008 e del 25/06/2009) i soggetti interni ed esterni all'Azienda che svolgono attività di gestione e manutenzione di impianti di elaborazione o di sue componenti nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;

Tenuto conto che è in fase di ultimazione la ricognizione - a cura del Responsabile della Protezione dei Dati - volta ad individuare correttamente:

a) i soggetti esterni le cui attività presuppongono la designazione a Responsabile dei Trattamenti ai sensi dell'art. 28 del GDPR;
b) i soggetti esterni che svolgono attività che presuppongono la nomina di Amministratore di Sistema;

Considerato che è necessario individuare un supporto tecnico-amministrativo aziendale al Responsabile della Protezione Dati, i cui compiti sono di seguito indicati, la cui attività cesserà contestualmente alla cessazione dell'incarico di RPD da parte dell'ing. Gianfranco Bruno;

Ritenuto che si debba procedere attraverso una pianificazione certa alla traduzione delle indicazioni che il RPD fornirà nell'ambito delle responsabilità, competenze tecniche e amministrative delle Strutture preposte, partendo dalla rilevazione dell'attuale stato dell'arte per arrivare alla piena attuazione della vigente normativa in materia di protezione dei dati personali;

Dato atto che la formulazione della proposta di un atto deliberativo impegna la responsabilità del soggetto proponente in ordine alla regolarità amministrativa e legittimità del contenuto della stessa;

Acquisiti i pareri favorevoli del Direttore amministrativo, del Direttore sanitario, resi per quanto di rispettiva competenza;

Dato atto che la formulazione della proposta di un atto deliberativo impegna la responsabilità del soggetto proponente in ordine alla regolarità amministrativa e legittimità del contenuto della stessa;

PROPONE AL DIRETTORE GENERALE

Di adottare l'adeguamento dell'organizzazione privacy nell'Ente secondo le previsioni dell'art. 2-quatordecies del D. Lgs. 101/2018 attribuendo specifici compiti e funzioni connessi al trattamento di dati personali così come previsti dalle normative vigenti;

- **di rilevare** che l'adeguamento organizzativo di cui trattasi potrà essere modificato e/o integrato in applicazione degli indirizzi forniti dall'RPD-ASP;

IL DIRETTORE GENERALE

In virtù dei poteri conferitigli con Decreto di nomina dal Presidente della Giunta Regionale di Basilicata n. 258 del 16.11.2018;

Letta e valutata la proposta deliberativa riportata in narrativa;

Acquisiti i pareri favorevoli del Direttore amministrativo, del Direttore sanitario, resi per quanto di rispettiva competenza;

DELIBERA

di adottare la proposta di deliberazione sopra riportata, nei termini indicati e per l'effetto:

1. richiamare le motivazioni espresse in premesse;
2. prendere atto della nomina a Responsabile della Protezione dei Dati (RPD) conferita con Delibera Commissariale n. 537/2018 all'ing. BRUNO Gianfranco;
3. designare quali persone fisiche cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali i dirigenti responsabili di Strutture Semplici (anche Dipartimentali) e di Strutture Complesse, ai quali verrà notificata la designazione secondo il modello di cui all'allegato 2, parte integrante e sostanziale del presente atto;
4. autorizzare i dipendenti assegnati alle strutture e i soggetti che vi operano a qualsiasi altro titolo al trattamento dei dati personali, nel rispetto del principio di minimizzazione dei dati, secondo le istruzioni riportate nell'allegato 1), parte integrante e sostanziale del presente atto, stabilendo che l'ambito di trattamento di ciascun autorizzato (tipi di dati personali trattati, operazioni di trattamento eseguibili, banche dati accessibili ecc.) verrà individuato con apposito successivo provvedimento del Direttore Generale;
5. individuare quali Responsabili dei Trattamenti i soggetti che effettuano Trattamenti di dati personali per conto della ASP; tali soggetti verranno indicati dal RPD a conclusione della rilevazione in corso di ultimazione e con essi verrà sottoscritto apposito accordo secondo il modello di cui all'allegato 3 parte integrante e sostanziale del presente atto;
6. dare mandato alla UOC Sistema informativo Aziendale di individuare gli Amministratori di sistema interni all'Azienda; per quanto riguarda gli esterni, il DPO - a conclusione della rilevazione in corso di ultimazione – comunicherà alla UOC Sistema informativo Aziendale l'elenco dei fornitori che svolgono attività da Amministratori di Sistema e le relative funzioni svolte;
7. prendere atto della esistenza del Registro delle attività di trattamento dando mandato alle strutture competenti di mantenerlo costantemente aggiornato in tempo reale;
8. stabilire che ogni struttura – sin dalla fase di predisposizione dei documenti di gara – deve segnalare al RPD la possibilità che l'oggetto della gara possa comprendere trattamento di dati personali per conto dell'Azienda rientrando quindi nel novero dell'art. 28 del Regolamento UE in base al quale il futuro contraente dovrà ricoprire il ruolo di Responsabile dei Trattamenti; la struttura che effettua la segnalazione collaborerà con il DPO per la redazione dello schema di accordo per la designazione a Responsabile dei Trattamenti che deve costituire parte integrante dei documenti di gara;
9. dare mandato alla UOC Sistema informativo Aziendale di aggiornare - con la consulenza del RPD e con la piena e fattiva collaborazione delle altre Strutture interessate - le linee guida relative all'utilizzo delle risorse informatiche aziendali (hardware, software, reti, infrastrutture ecc.) sulla base delle indicazioni contenute nell'allegato 1 succitato;
10. individuare quale supporto tecnico-amministrativo aziendale al Responsabile della Protezione Dati la U.O.S.D. Trasparenza, alla quale verranno assegnate risorse umane e strumentali in base alle necessità segnalate, la cui attività cesserà contestualmente alla cessazione dell'incarico di RPD da parte dell'ing. Gianfranco Bruno;
11. demandare alla U.O.S.D. Trasparenza il compito di:
    - formalizzare e sottoscrivere le designazioni predisposte e approvate dall'RPD ai soggetti di cui al punto 3 del presente provvedimento secondo l'allegato 2, parte integrante e sostanziale del presente atto;

- formalizzare e sottoscrivere gli accordi predisposti ed approvati dall'RPD con i soggetti di cui al punto 5 secondo l'allegato 3 parte integrante e sostanziale del presente atto;

12. demandare al Responsabile della UOC Sistema informativo Aziendale il compito di formalizzare e sottoscrivere l'incarico di Amministratore di Sistema predisposto ed approvato dall'RPD ai soggetti interni ed esterni secondo lo schema dell'allegato 4, parte integrante e sostanziale del presente atto;
13. dare mandato al RPD, con la collaborazione di tutte le strutture, di individuare gli ambiti di trattamento consentiti ai soggetti autorizzati di cui al punto 4), la cui declaratoria verrà approvata con apposito provvedimento del Direttore Generale.
14. Approvare gli allegati indicati in narrativi ovvero:
    - Allegato 1: Istruzioni agli autorizzati al trattamento dei dati personali
    - Allegato 2: Designazione persone fisiche per specifici compiti e funzioni
    - Allegato 3: Accordo con fornitori per incarico di Responsabili del Trattamento
    - Allegato 4: Nomina Amministrazioni di sistema

- revocare le Delibere del Direttore Generale n. 10/2011 e 251/2011 con cui venivano nominati i Responsabili dei Trattamenti di Dati Personali ai sensi dell'art. 29 del D.Lgs. 196/2003;

- la presente deliberazione non comporta impegni di spesa;

- trasmettere la presente Deliberazione all'Ing. Gianfranco Bruno, R.P.D. – ASP di Potenza per i seguiti di competenza.

ALLEGATO 1

ISTRUZIONI AGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Nelle more dell'emanazione di apposite linee guida a cura della Struttura Innovazioni Tecnologiche ed Attività Informatiche, il trattamento dei dati da parte dei dipendenti e degli altri soggetti autorizzati dovrà avvenire nel rispetto dei principi del Regolamento (UE) 2016/679 (cd. GDPR), del Decreto Legislativo n. 101/2018 e delle ulteriori disposizioni impartite.

L'accesso ai dati è consentito per quanto strettamente necessario per adempiere ai compiti individualmente assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata dal titolare del trattamento.

In particolare, per quanto riguarda le elaborazioni e le altre fasi dei trattamenti effettuate attraverso i personal computer collegati alla rete aziendale, ciascun autorizzato disporrà di credenziali personali.

Gli autorizzati avranno cura di:

- non condividere le proprie credenziali con altri utenti (a meno che non sia espressamente previsto);
- non cedere a terzi le proprie credenziali di accesso;
- non accedere a servizi loro non consentiti;
- non caricare ed eseguire software di rete o di comunicazione senza previa verifica dello stesso da parte del referente informatico;
- non tentare di acquisire privilegi di amministratore di sistema;
- non collegare modem o altri dispositivi che consentano un accesso non controllato ad apparati della rete della ASM;
- effettuare il backup periodico dei propri dati di interesse.

Per quanto riguarda la eventuale documentazione cartacea, atti e documenti contenenti i dati devono essere custoditi a cura degli operatori per la durata del trattamento e successivamente conservati in archivi ad accesso controllato, secondo quanto sarà indicato di volta in volta.

Nel caso di trattamento di dati particolari o di dati giudiziari, gli atti e i documenti contenenti i dati affidati agli autorizzati del trattamento devono essere conservati in contenitori muniti di serratura.

Gli autorizzati sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto.

Analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici aziendali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

ALLEGATO 2 – Attribuzione compiti e funzioni

Prot. n. _____
Data: _____

Al dott. _____
Dirigente Struttura _____

Oggetto: Regolamento UE 2016/679 – D. Lgs. N. 101/2018 - Attribuzione di specifici compiti e funzioni connessi al trattamento di dati personali.

In esecuzione della Delibera Commissariale n. _____ del _____, ai sensi dell'art. Art. 2-quaterdecies – par. 1 del D. Lgs. 101/2018, l'Azienda Sanitaria di Potenza, Titolare del trattamento dei dati personali, le conferisce i seguenti specifici compiti e funzioni connessi al trattamento di dati personali nell'ambito della Struttura in capo alla S.V.:

1. sorvegliare affinchè siano ridotti al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, nonché i rischi di distruzione o perdita, anche accidentale, dei dati personali stessi, e più in generale vengano rispettati i principi generali contenuti nell'art. 5 del Regolamento UE;
2. accertarsi che i soggetti facenti parte della struttura in capo alla S.V. svolgano i trattamenti di dati nel rispetto degli ambiti di trattamenti individuati con Delibera del _____ Commissario/Direttore Generale n. ___ del _____; per casi particolari la S.V. ha facoltà di integrare o modificare gli ambiti di trattamento individuati con la Delibera suddetta;
3. curare che ai soggetti interessati (ovvero a coloro i cui dati vengono trattati nell'ambito della Struttura da Lei diretta) venga erogata l'Informativa prevista secondo i modelli forniti dall'Azienda e che da parte degli stessi - nei casi previsti - venga acquisito il consenso al trattamento;
4. avvertire immediatamente il Responsabile della Protezione dei Dati (RPD) di ogni richiesta, provvedimento, accertamento, controllo da parte del Garante o dell'Autorità giudiziaria;
5. avvertire immediatamente il RPD di eventuali violazioni di dati (cd. Data Breach) che si dovessero verificare nell'ambito della Struttura;
6. più in generale segnalare al RPD il verificarsi di qualsiasi evento in qualche modo correlato alla protezione dei dati personali;
7. coinvolgere il RPD in qualsiasi attività con rilevanza privacy da mettere in atto; a titolo esemplificativo, ma non esaustivo, potrebbe trattarsi dell'attivazione di un nuovo software, dell'attivazione di procedura concorsuale o procedura di gara per fornitura di servizi o attivazione di una collaborazione con soggetti terzi, anche a titolo non oneroso;
8. curare la diffusione ed il rispetto delle istruzioni che il Titolare – anche per il tramite del RPD - vorrà impartire in ordine ad aspetti connessi con la protezione dei dati personali nonché di regolamenti e/o provvedimenti adottati a livello aziendale per la protezione dei dati personali.

È opportuno rammentare che l'attribuzione di specifici compiti e funzioni connessi al trattamento di dati personali non libera il Titolare dalla cura e dalle responsabilità che la disciplina sulla Protezione dei Dati Personali attribuisce al Titolare, e pertanto l'attribuzione di tali compiti e funzioni a soggetti diversi non costituisce 'assunzione' di doveri sottratti al Titolare bensì affiancamento e condivisione di tali doveri; pertanto, a titolo esemplificativo, in capo ai soggetti designati - non titolari di budget specifico - non grava alcun obbligo di procurarsi strumenti e/o risorse di cui non dispongono: essi sono piuttosto tenuti a far rispettare 'per quanto possibile' le norme esistenti o appositamente emanate, segnalando anzi al Titolare fabbisogno di risorse strutturali aggiuntive o situazioni di rischio specifico da sanare, fermo restando l'obbligo dell'attivazione di tutte quelle azioni, anche cruciali, che non presentano ostacoli di sorta né impegni economici.

La presente viene consegnata alla S.V. in duplice copia con preghiera di restituirne un esemplare espressamente datato e sottoscritto per ricezione.

IL DIRETTORE GENERALE

_____

Per ricezione:

_____

LI, _____

ALLEGATO 3 – Nomina Responsabili

AZIENDA SANITARIA LOCALE DI POTENZA

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI (ART. 28 DEL REGOLAMENTO UE 679/ 2016)

PREMESSA. A seguito dell'entrata in vigore del Regolamento EU 2016/679 in materia di protezione dei dati personali (GDPR), poiché il servizio di _____ svolto dalla Ditta _____ a favore dell'Azienda Sanitaria di POTENZA (ASP) presuppone trattamenti di dati personali effettuati per conto dell'Azienda stessa, Titolare del trattamento, la Ditta _____ assume il ruolo di Responsabile del trattamento ai sensi dell'art. 28 del GDPR.

Ciò premesso, tra **la Azienda Sanitaria Locale di Potenza** (qui di seguito, '**Titolare'**), con sede legale in Potenza Via Torraca 2, rappresentata da _____,

e

la Ditta **_____** (qui di seguito, '**Responsabile'**), con sede legale in _____, rappresentata da _____,

si conviene e stipula quanto riportato nel presente accordo:

1. **Oggetto**

Oggetto del presente accordo è la definizione delle modalità con le quali il Responsabile del trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali definite di seguito.

Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione relativa al trattamento dei dati personali, ovvero il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, 'il Regolamento'), il D. Lgs. 101/2018 ed i Provvedimenti Generali che il Garante per la Protezione dei Dati Personal) adotterà in attuazione delle prescrizioni del medesimo D. Lgs. 101/2018.

2. **Descrizione delle prestazioni del Responsabile del trattamento**

Il Responsabile del trattamento è autorizzato a trattare per conto del Titolare i dati personali necessari per fornire il servizio di _____
_____
_____.
Si da atto che tra i dati personali trattati vi sono/non vi sono dati particolari (di cui all'art. 9 del Regolamento) e/o dati afferenti a reati o condanne penali (di cui all'art. 10 del Regolamento).
Le persone interessate ai trattamenti sono:

- gli utenti dell'Azienda Sanitaria nonché loro parenti, tutori, procuratori, amministratori di sostegno e più in generale le persone che si prendono cura di soggetti non in dotate di autonomia decisionale;
- dipendenti e assimilati (interinali, stagisti, tirocinanti, collaboratori esterni, consulenti ecc.);
- fornitori;
- _____

3. **Durata del contratto**

Il presente contratto entra in vigore a partire dalla data di sottoscrizione del presente accordo e cesserà contestualmente alla cessazione del contratto di servizio. Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, quest'ultimo sarà tenuto a restituire al Titolare i dati personali oggetti del trattamento oppure a provvedere, previo avviso

scritto, alla loro integrale distruzione salvo i casi in cui la conservazione dei dati sia richiesta da norme di legge.

4. Obblighi del Titolare del trattamento

Il Titolare del trattamento s'impegna a:

- Fornire al Responsabile i dati necessari per consentire le attività fornendogli al contempo le istruzioni necessarie;
- Vigilare durante la durata del contratto sul rispetto - da parte del Responsabile - degli obblighi previsti dal Regolamento.

5. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento si impegna a:

a) Trattare i dati solo per le finalità sopra specificate nell'ambito dell'esecuzione delle prestazioni contrattuali di servizio.

b) Trattare i dati **conformemente alle normativa vigente in materia di Protezione dei dati personali** come descritta al punto I**.** Inoltre, se il Responsabile del trattamento è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.

c) Garantire la **riservatezza** dei dati personali trattati nell'ambito del contratto di servizio.

d) Controllare che le **persone designate e/o autorizzate a trattare i dati personali** in virtù del presente contratto:
   - Si impegnino a rispettare la **riservatezza** o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - Ricevano la **formazione** adeguata in materia di protezione dei dati personali.

   Se richiesto, il Responsabile fornisce al Titolare l'elenco delle persone fisiche designate o autorizzate ai trattamenti.

e) Tenere conto, utilizzando i materiali, i prodotti, le applicazioni od i servizi, dei principi di **protezione dei dati a partire da quando queste attività vengono progettate** e della **protezione dei dati di default.**

f) **Sub Responsabile del trattamento**
   Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "**sub-Responsabile**") per gestire attività di trattamento specifiche. In questo caso, informa in precedenza e per iscritto il Titolare di ogni cambiamento ravvisato riguardante l'aggiunta o la sostituzione di altri Responsabili. Questa informazione deve indicare chiaramente le attività di trattamento delegate, l'identità e gli indirizzi del sub-Responsabile del trattamento ed i dati del contratto di esternalizzazione. Il Titolare del trattamento dispone di un tempo massimo di 2 settimane a partire dalla data di ricevimento di questa informazione per presentare le proprie obiezioni: la collaborazione può essere attivata se il Titolare non ha posto obiezioni durante il tempo stabilito.
   Il sub-Responsabile deve rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del Titolare. Spetta al Responsabile iniziale assicurare che il sub-Responsabile presenti le

stesse garanzie sufficienti alla messa in opera di misure tecniche ed organizzative appropriate di modo che il trattamento risponda alle esigenze del Regolamento. Se il sub-Responsabile non adempisse alle proprie obbligazioni in materia di protezione dei dati, il Responsabile iniziale è interamente responsabile dell'esecuzione da parte del sub-Responsabile dei suoi obblighi rispetto al Titolare.

g) Diritto di informazione delle persone interessate.

Spetta al Titolare del trattamento fornire l'informativa di cui agli art. 13-14 alle persone interessate per le operazioni del trattamento al momento della raccolta dei dati.

h) Esercizio dei diritti delle persone

Per quanto possibile, il Responsabile deve assistere il Titolare del trattamento nell'espletamento dei propri obblighi di far seguito alle domande di esercizio dei diritti delle persone interessate: diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto a trasferire i dati, diritto di non essere oggetto di una decisione individuale automatizzata (compresa la profilazione). Qualora le persone interessate esercitino tale diritto presso il Responsabile, questi deve inoltrare la richiesta per posta elettronica al Responsabile della Protezione dei Dati del Titolare.

i) Notifica della violazione di dati a carattere personale

Il Responsabile informa il Titolare di ogni violazione di dati senza ingiustificato ritardo dopo esserne venuto a conoscenza; l'informazione è accompagnata da ogni documentazione utile per permettere al Titolare, se necessario, di notificare questa violazione all'Autorità di controllo competente e, se del caso, alle persone fisiche (interessati) vittime del data breach.

j) **Assistenza del Responsabile del trattamento nell'attuazione degli obblighi del Titolare del trattamento**

Il Responsabile assiste il Titolare nella realizzazione di analisi d'impatto relative alla protezione dei dati, conformemente all'articolo 35 del Regolamento; egli assiste il Titolare anche nella eventuale consultazione preventiva dell'Autorità, prevista dall'articolo 36.

k) Misure di sicurezza

Il Responsabile del trattamento s'impegna a mettere in opera le misure di sicurezza tecniche ed organizzative idonee a garantire un livello di sicurezza adatto al rischio, ivi compresi, fra gli altri, se ritenuti necessari:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

l) Disposizione al termine delle prestazioni contrattuali

Al termine della prestazione dei servizi comportanti il trattamento di questi dati, il Responsabile, a scelta del Titolare, s'impegna a:

- Distruggere tutti i dati a carattere personale o
- Rimandare tutti i dati a carattere personale al Titolare del trattamento o

- Trasferire i dati a carattere personale al nuovo Responsabile designato dal Titolare; il trasferimento deve essere accompagnato dalla distruzione di tutte le copie esistenti nei sistemi di informazione del Responsabile. In tutti i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione attestante che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di competenza del Titolare.

m) Responsabile della protezione dei dati

Qualora lo abbia designato ai sensi dell'art. 37 del Regolamento, il Responsabile comunica al Titolare il nome ed i dati del proprio Responsabile della protezione dei dati.

n) Registro delle attività di trattamento

Il Responsabile dovrà **tenere per iscritto un registro delle attività di trattamento** effettuate per conto del Titolare secondo le previsioni dell'art. 30 comma 2 del Regolamento; il registro dovrà comprendere:

- Il nome e i dati del Titolare per conto del quale effettua i trattamenti, degli eventuali Responsabili e, se applicabili, del Responsabile della protezione dei dati;
- Le categorie di trattamenti effettuati per conto del Titolare del trattamento;
- Se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo comma del regolamento europeo sulla protezione dei dati, i documenti che attestano l'esistenza di opportune garanzie;
- Per quanto possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative, compresi eventualmente:
  - La pseudonimizzazione e cifratura dei dati a carattere personale;
  - gli strumenti che permettono di garantire la segretezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
  - I mezzi che permettono di ristabilire la disponibilità dei dati personali e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
  - Una procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento.

o) Documentazione

Il Responsabile del trattamento metterà a disposizione del Titolare la **documentazione necessaria per dimostrare il rispetto di tutti gli obblighi** e per permettere la realizzazione di revisioni, comprese le ispezioni, da parte del Titolare o di un altro revisore incaricato, e contribuire a queste revisioni.

p) Nomina di Amministratore di sistema

(Inserire qualora il Contratto di servizio includa attività ricomprese tra quelle disciplinate dal Provvedimento Generale 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 - 27 novembre 2008" (in G.U. n. 300 del 24 dicembre 2008) e successive specifiche integrazioni).

Col presente accordo il Responsabile assume funzioni di Amministratore di sistema esterno come da Provvedimento Generale 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 - 27 novembre 2008" (in G.U. n. 300 del 24 dicembre 2008) e successive specifiche integrazioni, avendo il Titolare valutato caratteristiche di esperienza,

capacità e affidabilità del Responsabile, che fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il Responsabile dovrà:

- curare un sistema di registrazione degli accessi al sistema informativo del Titolare da parte dei propri dipendenti o collaboratori, in modo che le registrazioni (access log) contengano i riferimenti dell'utente che ha avuto accesso, i dati temporali e la descrizione dell'evento che le ha generate e siano conservate con modalità che ne garantiscono l'immodificabilità;
- attenersi all'applicazione delle misure organizzative, fisiche, procedurali e logiche sulla sicurezza con particolare riferimento a quanto specificato nell'art. 32 del Regolamento 679/16 funzionali al raggiungimento di obiettivi di sicurezza adeguati;
- adottare "appropriate misure tecniche e organizzative" per assicurare "un livello di sicurezza adeguato al rischio " (art. 32, comma 1) rispetto a tipologia e mole di dati trattati;
- comunicare immediatamente al Titolare, e comunque non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante per la protezione dei dati personali o dell'Autorità Giudiziaria, ai sensi degli articoli 152 e da 157 a 160 del D.Lgs. 196/2003 come modificati dal D. Lgs. 101/2018;
- rispondere tempestivamente ed in modo esaustivo alle richieste e ai questionari eventualmente inviati dal Titolare per monitorare e vigilare sulle misure di sicurezza poste in essere e, più in generale, sull'applicazione del Reg. 679/16;
- Se richiesto, fornire al Titolare l'elenco delle persone che materialmente svolgono le funzioni connesse con le mansioni a ciascuno attribuite.

Potenza, _____

Firme: Il Titolare _____

Il Responsabile _____

AZIENDA SANITARIA LOCALE DI POTENZA

NOMINA DI AMMINISTRATORE DI SISTEMA

VISTO:

- il provvedimento del Garante per la protezione dei dati personali datato 27 novembre 2008, pubblicato sulla Gazzetta ufficiale n. 300 del 24 dicembre 2008, recante il titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- il provvedimento datato 12 febbraio 2009 pubblicato sulla G.U. n. 45 del 24 febbraio 2009, con il quale il Garante ha differito l'adozione delle misure relative alla nomina degli amministratori di sistema al 30 giugno 2009;
- la consultazione pubblica avviata dal Garante con deliberazione del 21 aprile 2009, pubblicata sulla G.U. n. 105 dell'8 maggio 2009;
- il provvedimento recante data 25 giugno 2009 pubblicato sulla Gazzetta Ufficiale n. 149 del 30 giugno 2009 con il quale il Garante ha parzialmente modificato ed integrato le disposizioni di cui al provvedimento emesso in data 27 novembre 2008.

CONSIDERATO CHE:

la qualifica e le prestazioni effettuate in favore della ASP forniscono idonea garanzia circa il pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo della sicurezza,
la S.V. / la Ditta _____ viene nominata AMMINISTRATORE DI SISTEMA in riferimento alle mansioni appresso indicate:

_____;
_____;
_____.

In virtù di tale nomina dovrà:

- trattare i dati personali di cui verrà a conoscenza in esecuzione dell'incarico ricevuto in conformità al contratto in essere e in ossequio alla vigente normativa in materia di privacy;
- *(in caso di nomina di persone giuridiche)* conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte;
- operare solo ed esclusivamente al fine di porre in essere le attività connesse all'attuazione delle obbligazioni di cui al contratto in essere con la ASP ed in particolare (*):

1. *manutenzione della rete dati LAN*
2. *gestione degli accessi alla rete LAN;*
3. *gestione degli account di posta elettronica;*

4. *gestione dei firewall e degli antivirus presenti presso l'azienda sanitaria;*
5. *supporto tecnico per la risoluzione delle problematiche inerenti i collegamenti LAN/WAN;*
6. *interfaccia con i fornitori e i manutentori dei servizi di fonia per la risoluzione di problematiche tecniche;*
7. *consulenza informatica ed interfaccia con i fornitori dei pacchetti hardware e software dell'azienda sanitaria;*
8. *manutenzione dei vostri server, controllo ed esecuzione delle procedure relative all'effettuazione delle copie di backup dei dati in collaborazione con le ditte fornitrici dei pacchetti software*
9. *predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici nella Sua qualità di amministratore di sistema. Tali registrazioni (access log) devono avere caratteristiche di completezza e inalterabilità, nonché possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per il quale sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a sei mesi.*

In ottemperanza alle norme vigenti, Vi ricordiamo che l'operato svolto in qualità di amministratore di sistema è soggetto a verifica ad opera del Titolare al fine di controllarne la conformità e la piena rispondenza alle misure organizzative, tecniche e di sicurezza adottate dalla ASP, a protezione dei dati personali trattati nell'esercizio delle attività istituzionali. Vi ricordiamo, altresì, che gli estremi identificativi della Ditta saranno resi noti, tramite l'informativa di cui all'art. 13 del Regolamento UE 2016/679, o tramite ordini o circolari interni di servizio, al personale in forza alla ASP, attesa la possibilità di accedere a sistemi e servizi che permettono il trattamento di informazioni di carattere personale dei lavoratori.

La presente viene consegnata alla S.V. in duplice copia con preghiera di restituirne un esemplare espressamente datato e sottoscritto per accettazione.
La nomina è efficace tra le parti fino alla scadenza e/o alla risoluzione del contratto in essere.

Il Titolare del trattamento dei dati personali — L'Amministratore di sistema

Dr. _____ — _____

Potenza, _____

(*) depennare le voci non interessate ed aggiungere altre non ricomprese nell'elenco

L'Istruttore

Il Responsabile Unico del Procedimento

Antonio Bavusi

Il Dirigente Responsabile dell'Unità Operativa

Il presente provvedimento è notificato ai destinatari a cura dell'istruttore.

Francesco Negrone	*Lorenzo Bochicchio*	*Vincenzo Andriuolo*
Il Direttore Sanitario Francesco Negrone	Il Direttore Generale Lorenzo Bochicchio	Il Direttore Amministrativo Vincenzo Andriuolo

Tutti gli atti ai quali è fatto riferimento nella premessa e nel dispositivo della deliberazione sono depositati presso la struttura proponente, che ne curerà la conservazione nei termini di legge.