Allegato al contratto n…….. del……
Privacy e le relative istruzioni per il trattamento

Il Titolare del Trattamento della Regione Basilicata, ai sensi dell'art. 29 del Regolamento UE 2016/679 (di seguito anche GDPR), al fine esclusivo di compiere le operazioni di trattamento di propria competenza, per lo svolgimento di attività inerenti alla manutenzione, il supporto operativo e l'assistenza specialistica per il Sistema Informativo SIRFO della Regione Basilicata ed alle linee d'intervento:

- LINEA 1) Manutenzione Adeguativa, Correttiva e Migliorativa (MAC) e Supporto Operativo (SO);
- LINEA 2)Manutenzione Evolutiva (MEV) e Servizio di consulenza specialistica (SC);

impartisce le seguenti direttive e istruzioni al Responsabile del Trattamento (Esterno) che presenta adeguata e documentata esperienza, capacità ed affidabilità in relazione ai compiti ad esso affidati, nonché idonea organizzazione tecnica, organizzativa e di risorse atte ad eseguirla.

Il Responsabile garantisce il rispetto delle vigenti disposizioni in materia di trattamento di dati personali, anche con riferimento al profilo relativo alla sicurezza (attraverso l'adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 32 del Regolamento UE 2016/679).

COMPITI E RESPONSABILITÀ

Il Responsabile offre al Titolare del trattamento il servizio di manutenzione, supporto operativo e assistenza specialistica del Sistema Informativo SIRFO della Regione Basilicata.

Tali servizi forniti ai sensi del contratto in questione. Nel periodo di vigenza contrattuale, il Responsabile esterno dovrà attenersi scrupolosamente alle presenti istruzioni e alle altre impartite dal Dirigente che ha sottoscritto il Contratto ovvero dal Data Protection Officer.

ISTRUZIONI IMPARTITE AL RESPONSABILE ESTERNO

Nello svolgimento dei suindicati compiti deve attenersi alle istruzioni impartite dal titolare e, in particolare, deve:

- trattare i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato;
- trattare tali dati solo per finalità determinate, esplicite e legittime indicate dal Titolare, e successivamente trattarli in modo compatibile con tali finalità;
- verificare che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità definite dal Titolare per le quali sono trattati;
- conservare e trattare i dati personali solo in base alle istruzioni ricevute e non per altre finalità;
- trattare i dati in modo integro e riservato garantendo, per quanto di propria competenza, un'adeguata sicurezza degli stessi in modo da ridurre il rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- trattare i dati, su indicazione del Responsabile del trattamento, sulla base di un obbligo legale oppure del consenso dell'interessato oppure per l'esecuzione di un contratto di cui l'interessato è parte oppure per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica oppure per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento oppure per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a

condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;

- comunicare i dati personali dell'interessato solo previa autorizzazione del Titolare e/o del Responsabile del Trattamento;
- accertarsi, ogni qualvolta si raccolgano dati personali, che venga fornita l'informativa ai soggetti interessati.
- assicurarsi che ogni comunicazione avvenga esclusivamente per finalità collegate all'esecuzione del contratto in essere con il Titolare del trattamento.

E ancora, il Responsabile esterno dovrà:

- cooperare con il Titolare e Responsabile del Trattamento per garantire agli interessati, per quanto di propria competenza, un effettivo ed efficace esercizio dei diritti di cui agli artt. 15 e successivi del Regolamento;
- designare per iscritto gli Autorizzati al trattamento dei dati personali che svolgeranno operazioni di trattamento, impartendo agli stessi le necessarie istruzioni e verificando che queste siano rispettate;
- svolgere formazione periodica agli Autorizzati al trattamento dei dati personali relativamente alle tematiche connesse alla protezione dei dati personali;
- nominare i designati al trattamento di cui al D.lgs 101/2018 art 2-quaterdecies, verificarne l'attività e conservare l'elenco contenente gli estremi identificati degli stessi, con l'indicazione delle funzioni ad essi attribuite, in conformità con la normativa vigente; (ad esclusione delle attività di competenza del Centro Tecnico Regionale);
- consegnare l'elenco degli amministratori di sistema di cui al punto precedente al titolare e/o Responsabile del trattamento e comunicare tempestivamente allo stesso ogni suo mutamento;
- implementare e verificare l'adozione delle misure tecniche ed organizzative previste per legge o regolamento e comunque di quelle volte a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei dati, dei servizi e dei sistemi impiegati durante le operazioni di trattamento, garantendo un elevato standard di sicurezza e protezione dei dati;
- predisporre una procedura interna atta all'identificazione delle violazioni dei dati personali (come definito nell'Articolo 4 del Regolamento) e comunicare con prontezza, e comunque entro 48h dall'identificazione di detta violazione, al Titolare e/o Responsabile del trattamento, fornendo le opportune informazioni;
- comunicare con prontezza qualsiasi circostanza o evenienza rilevante ai fini del Regolamento UE n. 679/2016 (come richieste del Garante, ispezioni, violazioni di dati, ecc.), nonché l'esito della procedura suddetta e qualsiasi violazione dei dati personali;
- conservare separatamente da altri dati personali i dati idonei a rivelare lo stato di salute o la vita sessuale o dati giudiziari trattati per finalità che non richiedono il loro utilizzo;
- ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;
- se il trattamento di dati è effettuato in violazione dei principi già menzionati è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Il Responsabile esterno deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali.

In ogni caso la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito alla responsabilità civile, si fa rinvio all'art. 154 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

FACOLTÀ E DOVERI DEL RESPONSABILE DEL TRATTAMENTO ESTERNO

Il Responsabile esterno:

- garantisce al Titolare che gli Autorizzati al trattamento dei dati personali da lui designati sono vincolati al più stretto riserbo sulla base di atti negoziali (es. codici di condotta interni, accordi di riservatezza specifici (NDA), ecc.) o disposizioni normative previste dal diritto dell'Unione o dal diritto nazionale cui il Fornitore/Responsabile Esterno e gli Autorizzati al trattamento dei dati personali sono soggetti.
- potrà avvalersi di un altro soggetto per lo svolgimento di parte delle attività di trattamento a lui delegate (cosiddetto "sub-responsabile") previa autorizzazione scritta, specifica o generale da parte del Titolare del trattamento. L'incarico conferito dovrà essere disciplinato da un atto di designazione a responsabile del trattamento conforme a quanto previsto dall'Articolo 28, comma 2 e 4, del Regolamento UE 679/2016. In caso di autorizzazione scritta generale, il Responsabile dovrà informare il Titolare di eventuali designazioni o sostituzioni dei sub-responsabili del trattamento; il Titolare si riserva la facoltà di opporvisi nel termine di 30 giorni dal momento in cui viene informato della circostanza da parte del Responsabile.
- risponde dei danni causati nel corso delle operazioni di trattamento dall'operato dei soggetti da lui autorizzati, fatto salvo il diritto di rivalersi nei loro confronti.

Nel caso in cui il Responsabile esterno trasferisca i dati personali trattati verso un Paese terzo o un'Organizzazione internazionale per adempiere ad un obbligo giuridico di cui è soggetto dovrà informare della circostanza il Titolare prima dell'inizio delle attività di trattamento o del trasferimento stesso, salvo che ciò sia vietato da rilevanti motivi d'interesse pubblico o obblighi di legge o regolamento.

È dovere del Responsabile esterno assistere il Titolare del trattamento, con misure tecniche e organizzative adeguate, nell'adempimento dei suoi obblighi di riscontro alle richieste degli interessati, sia fornendo allo stesso tutte le informazioni e i dati in suo possesso, sia adoperandosi materialmente per consentire al Titolare di dar seguito alle istanze ricevute. Qualora l'implementazione di dette misure di sicurezza tecniche e organizzative rientrino nell'ambito degli obblighi contrattuali il Responsabile esterno provvede direttamente ad effettuarne l'implementazione dandone comunicazione al Titolare. Qualora, invece, queste non rientrino nell'ambito contrattuale in essere, provvede in ogni caso a comunicare al Titolare la necessità di provvedere all'implementazione, fornendo le opportune informazioni per valutarne i costi.

Analogamente, è dovere del Responsabile esterno, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, assistere il Titolare sia nell'adempimento degli obblighi in materia di misure di sicurezza che nello svolgimento di una consultazione preventiva presso l'Autorità di controllo ai sensi dell'Articolo 36 del Regolamento UE 679/2016.

Alla scadenza del contratto di servizi, indicato precedentemente, qualora non rinnovato, il Fornitore/Responsabile esterno dovrà restituire al Titolare tutti i dati personali elaborati per suo conto e cancellarli in modo permanente dai sistemi informativi nella sua disponibilità, salvo che lo stesso non sia soggetto a specifici obblighi di conservazione ai sensi di legge o regolamento.

Qualora richieste, il Fornitore dovrà consegnare al Titolare tutte le informazioni necessarie a dimostrare l'ottemperanza agli obblighi previsti dal presente atto di designazione e dalla normativa vigente.

FACOLTÀ E DOVERI DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento si riserva il diritto di aggiornare i compiti e le istruzioni impartite al Fornitore/Responsabile esterno o di assegnarne di nuovi.

Il Titolare del trattamento, inoltre, si riserva il diritto di eseguire controlli, attraverso ispezioni o attività di audit, sull'effettivo svolgimento delle attività e dei compiti affidati al Fornitore. Infine, il Titolare verificherà periodicamente la sussistenza dei caratteri di esperienza, capacità ed affidabilità in capo al Fornitore e il rispetto da parte dello stesso di tutte le disposizioni normative in materia di sicurezza dei dati. A tal fine il Titolare potrà richiedere al Fornitore di essere relazionato per iscritto attraverso regolari report.

È onere del Titolare, in ogni caso, quello di tenere informato e aggiornare il Fornitore/Responsabile esterno di qualsiasi circostanza rilevante ai fini dell'attività di trattamento a lui delegate.

Il presente atto di designazione ha durata pari alla durata del contratto e si intende concluso allo scadere naturale dello stesso ovvero allo scadere dell'estensione del contratto stesso. Il presente atto di designazione si intende revocato allo scioglimento, per qualsiasi causa, del medesimo vincolo legale.

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

INFORMAZIONI E ISTRUZIONI AGLI AUTORIZZATI

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali D.Lgs 196/03 e s.m.i. recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 (RGPD) ed in relazione alle attività svolte nell'ambito istituzionale l'*autorizzato*, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal *Titolare del Trattamento* o dal *Designato al Trattamento* presso il quale opera. I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;
b) in modo lecito e secondo correttezza;
c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d) nel pieno rispetto delle misure di sicurezza definite, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure di sicurezza definite sono obbligatorie, e sono state anche distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **Con l'ausilio di strumenti elettronici** (es. PC, notebook, tablet o smartphone);
2. **Senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporti magnetici/ottici);
3. **Di carattere generale.**

Trattamenti dati con Strumenti Elettronici

Gli autorizzati al trattamento dovranno attenersi alle seguenti misure di sicurezza:

- accedere ai sistemi informativi esclusivamente per mezzo di credenziali di autenticazione personali; le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'autorizzato, associato ad una parola chiave (password) conosciuta solo dall'autorizzato;
- utilizzare la password con una lunghezza minima di otto caratteri, composte sia da numeri che lettere e caratteri speciali (o, se il sistema informativo in uso non lo permette, dal numero massimo di caratteri consentito) e differente dallo user id;
- ove non definito dall'Amministratore della rete, nella generazione della password non utilizzare elementi o notizie facilmente riconducibili all'autorizzato e non utilizzare password simili alla precedente;
- ove non definito dall'Amministratore della rete, modificare la password al primo utilizzo del sistema informativo, quindi ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono particolari - ad. es. di salute - e/o giudiziari) e nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, provvedere autonomamente a tale variazione;

- adottare particolari cautele per assicurare la segretezza della password (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi) custodendola con diligenza e riservatezza;
- per le banche dati automatizzate che utilizzano il proprio codice di accesso personale, evitare di operare su altre postazioni di lavoro al fine di non incorrere in trattamenti non autorizzati;
- tenere un comportamento corretto durante la navigazione in internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete e non è consentito navigare sui siti web non attinenti allo svolgimento delle mansioni assegnate;
- non aprire messaggi di posta provenienti da soggetti esterni *non accreditati* e non utilizzare l'indirizzo di posta elettronica istituzionale per fini personali;
- non comunicare la mail istituzionale a siti per i quali non siete interessati per fini lavorativi;
- non trasmettere dati particolari (ex sensibili) via e-mail. Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;
- bloccare la propria postazione di lavoro informatica durante la pausa pranzo, ovvero in tutte le occasioni in cui ci si assenti o ci si allontani anche temporaneamente dalla propria postazione di lavoro; nel caso in cui fosse necessario mantenere accesa la postazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;
- adottare tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento anche cartaceo a dipendenti o altri autorizzati;
- non lasciare la propria stazione di lavoro incustodita e collegata alla rete e/o ai sistemi informativi con il proprio account (nome utente) e password;
- non alterare in alcun modo la configurazione software della postazione di lavoro, evitando di installare qualunque software sconosciuto o non autorizzato dal competente reparto ICT;
- non utilizzare la rete dell'Amministrazione per fini personali e non espressamente autorizzati.

Trattamenti senza l'ausilio di Strumenti Elettronici

Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- garantire sempre la corretta custodia dei dati personali; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri autorizzati addetti al medesimo trattamento; non devono essere altresì consultati da altri autorizzati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
- per il tempo necessario allo svolgimento delle operazioni di trattamento, si dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati; conservare i documenti o gli atti che contengono dati particolari (ex dati sensibili) e/o giudiziari in archivi ad accesso controllato (armadi/schedari/contenitori chiusi da apposita serratura oppure soggetti a sorveglianza da parte di personale preposto);
- al termine delle operazioni di trattamento, restituire tempestivamente la documentazione prelevata dagli archivi ed assicurarsi che questa venga opportunamente riposta;
- in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola postazione di lavoro, le stampe devono essere o immediatamente raccolte e custodite con le modalità sopra descritte; Qualora i documenti da stampare contengano dati particolari è necessario, nei limiti del possibile, presenziare la fase di stampa o utilizzare la modalità di stampa protetta;
- non gettare via copie cartacee contenenti dati personali, senza averle prima distrutte in modo opportuno o comunque avere reso l'identificazione dell'interessato impossibile;
- adottare misure che siano idonee a limitare la conoscenza dei dati personali e/o particolari qualora essi siano presenti nei flussi documentali dell'amministrazione garantendo il rispetto della riservatezza dei dati degli interessati, ad esempio riponendo, i documenti in cassetti o armadi debitamente chiusi a chiave.
- è assolutamente vietato cedere a soggetti esterni i dati personali di cui si è venuti a conoscenza durante lo svolgimento dell'incarico.

Misure di carattere generale

Gli autorizzati al trattamento dovranno attenersi alle seguenti istruzioni:

- assicurare la riservatezza opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del RGPD e del D.lgs 196/2003 e s.m.i.;
- assicurare la somministrazione dell'informativa al trattamento dati ogni qual volta venga coinvolto un nuovo interessato;
- assicurarsi, quando previsto, che sia stato rilasciato il consenso al trattamento dati da parte dell'interessato;
- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall'Amministrazione;

- è consentita la trasmissione di dati all'interno dell'Amministrazione per i compiti ed i fini stabiliti dalla stessa per mezzo del Titolare, agendo sotto la sua diretta autorità, allo stesso modo sono autorizzati i trattamenti di dati pseudonimizzati;
- sono consentite le comunicazioni di dati personali che avvengono nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Amministrazione con terzi per l'esternalizzazione di attività/funzioni/servizi, a condizione che il terzo sia stato nominato Responsabile (esterno) del trattamento dei dati;
- è vietata ogni comunicazione/diffusione di dati verso l'esterno dell'Amministrazione senza preventiva autorizzazione; il divieto permane anche dopo la cessazione dell'incarico e/o del rapporto di lavoro;
- è vietato l'utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;
- è vietato raccogliere, registrare e conservare i dati personali presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- è vietato cedere ad altri dati personali di cui si è venuti a conoscenza durante lo svolgimento dell'incarico;
- è necessario astenersi dall'effettuare operazioni di trattamento dei dati personali, di cui si è venuti a conoscenza durante lo svolgimento dell'incarico, evitando di conservarli, duplicarli, comunicarli o cederli ad altri, dopo la cessazione del rapporto di lavoro;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- informare tempestivamente il proprio Dirigente di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;
- nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza e/o la riservatezza dei dati trattati, darne immediata comunicazione al proprio Dirigente;
- segnalare al proprio Dirigente eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire al Titolare o al Designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo e verifica di eventuali incidenti che possano essersi verificati;
- eseguire qualsiasi operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- recepire nuove indicazioni fornite dal Titolare del Trattamento o dal Designato anche partecipando a percorsi formativi quando previsti;
- trattare i dati personali, eventualmente riferiti a categorie particolari (art. 9) o relativi a condanne penali e reati (art. 10), è ammesso se lecito (art. 6) e cioè quando:
    - l'interessato ha espresso il consenso al trattamento dei propri dati personali;
    - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
    - il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;

o il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;

- garantire all'interessato l'esercizio dei diritti sui propri dati personali secondo quanto previsto dal Regolamento RGPD (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.) segnalando al proprio referente qualsiasi richiesta in questo senso.

Le presenti istruzioni rivestono carattere generale e sono suscettibili di essere integrate, specificate e aggiornate dal "Titolare" del trattamento dei dati, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali e pubblicate nella sezione "Trattamento dati personali e Privacy" nella intranet dell'Amministrazione.