



**Programma Regionale
FESR FSE+ Basilicata 2021-2027**

Codice CCI n. 2021IT16FFPR004
Decisione C (2022) 9766 del 16/12/2022

Allegato C
Incarico Responsabile trattamento esterno



Atto giuridico di nomina quale Responsabile del Trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE 2016/679 Disciplina dei trattamenti: compiti e istruzioni per il trattamento

TRA

La Regione Basilicata - Direttore Generale della Direzione Generale per la Salute e le Politiche della Persona – (di seguito denominata “Regione”), C.F. 80002950766, con sede in Potenza, viale Vincenzo Verrastro, 4, rappresentato dal Direttore Generale _____, nella persona di Direttore Generale pro tempore della Direzione Generale per la Salute e le Politiche della Persona, domiciliato per la carica presso la sede di cui sopra (D.G.R. n. _____), pec _____ (di seguito anche denominata “Titolare”);

e

_____, con sede legale in _____,
_____, P.Iva _____, pec
_____, nella persona del Direttore Generale e legale rappresentante
_____, (di seguito anche denominata “Responsabile” o
“_____”);

di seguito congiuntamente denominate “Parti”.

Premesso che:

- Le Parti hanno stipulato l'Accordo, rep. n. del, per l'attuazione del progetto “_____” teso a qualificare le competenze del personale sanitario” come indicato del “Piano” approvato con la deliberazione della Giunta regionale 29 giugno 2023, n. 387; (di seguito denominata “Accordo”),
- Nell'ambito delle attività dell'Accordo, _____ è preposto alle operazioni di trattamento dei dati personali di cui la Direttore Generale della Direzione Generale per la Salute e le Politiche della Persona è Titolare, qualificandosi, in tal modo, quale Responsabile del trattamento;
- In base all'art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (c.d. Regolamento Generale sulla Protezione dei Dati Personali, di seguito denominato “GDPR”) e alla normativa italiana di recepimento e di adeguamento, il Titolare del trattamento può nominare Responsabile del trattamento una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo selezionandolo tra soggetti che, per esperienza, capacità e affidabilità, forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali;

- _____ presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, in ordine all'adozione di misure tecniche e organizzative adeguate e assicura che il trattamento dei dati del Titolare avvenga nel rispetto dei principi definiti all'interno della normativa vigente in materia di protezione dei dati personali;
- In virtù delle attività affidate e del possesso delle suesposte qualità, il Titolare nomina _____ Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE 2016/679;

Il presente ATTO costituisce parte integrante e sostanziale dell'Accordo in essere tra le Parti.

Le Parti, sottoscrivendo il presente ATTO accettano e si impegnano a rispettare gli obblighi e le indicazioni in esso contenute.

Le Parti convengono, altresì, che le clausole contenute nel presente ATTO hanno prevalenza rispetto ad altri, diversi ed eventuali accordi correlati e inerenti gli stessi temi, vigenti al momento della sottoscrizione del presente ATTO;

Resta inteso che tale ATTO non comporta alcun diritto del Responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dalla qualifica a Responsabile, oltre quanto già previsto dall'Accordo di cui il presente ATTO costituisce integrazione;

Tutto ciò premesso, le Parti convengono quanto segue

Articolo 1 - Oggetto e conformità alla normativa vigente

1.1. Il presente ATTO è volto a disciplinare il trattamento di dati personali che il Responsabile effettuerà nell'ambito dell'esecuzione delle prestazioni indicate nell'Accordo stipulato con il Titolare.

1.2. Nel quadro delle loro relazioni, le Parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati personali e, in particolare, il Regolamento (UE) 2016/679 (c.d. Regolamento Generale sulla Protezione dei Dati Personali - GDPR) e il Codice Privacy 196/2003 come modificato dal D. Lgs. 101/2018.

1.3. Le attività di trattamento che il Responsabile potrà effettuare sono limitate a quelle strettamente necessarie ai fini dello svolgimento delle attività oggetto dell'Accordo, salvo ulteriori istruzioni da parte del Titolare del trattamento. In tal caso, il Titolare è tenuto a comunicare tali istruzioni in forma scritta e il Responsabile si riserva di svolgere una valutazione a livello progettuale ed economico in relazione alle stesse, prima della loro esecuzione.

Articolo 2 – Durata

2.1. Il presente ATTO seguirà la durata dell'Accordo in essere tra le Parti del quale è parte integrante e sostanziale.

2.2. In caso di risoluzione, recesso o cessazione dell'Accordo sottostante anche il presente ATTO perderà, pertanto, qualsivoglia efficacia.

Articolo 3 – Interessati e categorie di dati personali trattati

3.1. Il Responsabile è autorizzato a trattare, per conto del Titolare, dati a carattere personale necessari per fornire il servizio oggetto dell'Accordo.

3.2. Il Responsabile del trattamento è autorizzato dal Titolare a trattare le seguenti categorie di dati personali in relazione alle seguenti tipologie di interessati:

<i>Tipologia di dati personali</i>	<i>Categoria di interessati</i>
a) XXXXX	1) XXXXX

Articolo 4 - Misure di sicurezza

4.1. Il Responsabile si impegna a mettere in atto, in conformità con l'art. 32 GDPR, ogni misura di sicurezza idonea e adeguata a garantire la riservatezza dei dati trattati in esecuzione dell'Accordo, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illecito, o di trattamento non consentito o non conforme alle finalità della raccolta.

4.2 Nel caso in cui una delle Parti ritenesse insufficienti le misure di sicurezza in essere comunicherà per iscritto all'altra parte tale inadeguatezza, al fine di concordare e attuare ulteriori misure maggiormente idonee a prevenire incidenti di sicurezza. Il Responsabile del trattamento si riserva di svolgere una valutazione economico-progettuale prima dell'implementazione delle ulteriori misure di sicurezza richieste dal Titolare del trattamento.

4.3 Le misure di sicurezza tecniche e organizzative che il Responsabile si obbliga ad adottare sono le seguenti:

<u>Misure tecniche</u>	<u>Misure organizzative</u>
a) Scambio di informazioni attraverso protocolli sicuri (HTTPS).	1) Policy sulla protezione dei dati personali e sensibilizzazione costante sulle attività e gestioni degli apparati, applicativi e posta.
b) Sistemi antivirus/firewall.	2) Processi di gestione degli incidenti.
c) Procedure relative alle password (inclusi caratteri speciali, lunghezza minima, modifica obbligatoria della password alla data di scadenza stabilita).	3) Formazione degli Autorizzati.
d) Gestione centralizzata del sistema di accessi.	4) Istruzioni agli Autorizzati.
e) Diritti di accesso differenziati	
f) Misure di sicurezza dei software e cifratura dei dati	
g) Codifica mediante VPN per l'accesso remoto, il trasporto e la comunicazione dei dati.	

- h) Restare aggiornato su regole, norme o vulnerabilità relative alla sicurezza.
- i) Sviluppare e mantenere costantemente aggiornati gli standard di sicurezza.
- j) Sistemi di backup e recupero dati

4.4. Al Responsabile è conferita la facoltà di determinare le ulteriori misure di sicurezza, comunicate al Titolare, riguardanti gli aspetti più pratici del trattamento svolto per conto del Titolare.

Articolo 5 – Obblighi del Titolare

5.1. - Il Titolare garantisce che i dati da lui trasmessi al Responsabile sono raccolti rispettando ogni prescrizione della normativa vigente sul Trattamento dei dati personali, nonché pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati, in conformità con il principio di minimizzazione.

5.2. - Il Titolare del trattamento si impegna a documentare per iscritto e a garantire che tutte le istruzioni per il Trattamento dei dati personali in virtù della Accordo e del presente ATTO siano conformi alle norme di legge. Ogni variazione ritenuta necessaria dal Titolare nelle operazioni di trattamento dei dati, sarà comunicata ufficialmente dallo stesso al Responsabile.

5.3. - Il Titolare si impegna, inoltre, a vigilare, in anticipo e durante la durata di tutto il Trattamento, sul rispetto degli obblighi previsti dal Regolamento Europeo sulla Protezione dei Dati Personali da parte del Responsabile, nonché a fornire al Responsabile tutte le informazioni necessarie per identificare e valutare i rischi connessi al trattamento.

Articolo 6 – Obblighi del Responsabile

6.1. Il Responsabile si impegna:

- a trattare i dati personali degli interessati soltanto su istruzione documentata del Titolare;
- a garantire che le persone autorizzate al trattamento dei dati personali si siano impeginate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- ad adottare tutte le misure di sicurezza di cui all'art. 4 del presente ATTO;
- tenendo conto della natura del trattamento, ad assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del Regolamento UE 2016/679. In particolare si impegna a segnalare tempestivamente al Titolare l'eventuale esercizio dei diritti da parte degli interessati entro 48 h dalla ricezione della richiesta, senza rispondere autonomamente alla stessa;
- ad assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento UE 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione;

- tenere un registro, come previsto dall'art. 30 del GDPR di tutte le tipologie di attività di trattamento svolte per conto del Titolare in qualità di Responsabile;
- astenersi dal trattare dati personali oggetto della Accordo per finalità proprie;
- procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante Privacy del 27.11.2008, curando altresì l'applicazione di tutte le ulteriori prescrizioni in esso contenute;
- ad assistere il Titolare nella realizzazione di una valutazione d'impatto, qualora il trattamento possa presentare un rischio per i diritti e le libertà degli interessati;
- prima di procedere al trattamento, ad assistere il Titolare nell'adempimento dell'obbligo di consultazione dell'Autorità di controllo competente, qualora dalla valutazione d'impatto emerga che il trattamento comporti un rischio elevato per gli interessati;
- ad assistere il Titolare nell'adempimento dell'obbligo di garantire che i dati personali trattati siano esatti e aggiornati ed informare senza indugio il Titolare qualora venga a conoscenza del fatto che i dati che sta trattando sono inesatti o obsoleti;
- su richiesta del Titolare, a restituire tutti i dati personali trattati in esecuzione della Accordo dopo che è terminata la prestazione dei servizi relativi al trattamento e a cancellare le copie esistenti – dandone conferma scritta entro 30 giorni previa espressa richiesta del Titolare – salvo che il diritto dell'Unione Europea o italiano preveda la conservazione dei dati;
- a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente ATTO e all'art. 28 del Regolamento UE 2016/679 ed acconsente e si impegna a contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato, fermo restando che, in caso di sopralluoghi, (i) il Titolare dovrà dare al Responsabile un preavviso scritto di almeno 15 giorni lavorativi prima di ciascun controllo; (ii) le verifiche effettuate dal Titolare non potranno ostacolare la normale operatività del Responsabile. Le Parti concorderanno congiuntamente le modalità di svolgimento dell'attività di verifica e all'atto del preavviso il Titolare dettaglierà al Responsabile l'oggetto della stessa;
- ad informare immediatamente il Titolare qualora, a suo parere, un'istruzione violi il Regolamento UE 2016/679, il Regolamento UE 2018/1725 o altre disposizioni, nazionali o dell'Unione Europea, relative alla protezione dei dati;
- si impegna ad informare tempestivamente per iscritto il Titolare (e, in ogni caso, entro 48 ore ogniqualvolta venga a conoscenza o sospetti ragionevolmente che si sia verificato un incidente di sicurezza (c.d. DATA BREACH), tramite l'Allegato A al presente ATTO. La notifica dovrà avvenire tramite comunicazione inviata ai seguenti indirizzi e-mail/PEC del Titolare:
 - o P.E.C. E/O E-MAIL dg.sanita@cert.regione.basilicata.it
 - o - E-MAIL DEL FUNZIONARIO DELL'AMMINISTRAZIONE COMMITTENTE (in copia conoscenza) luciano.scavone1@regione.basilicata.it

Articolo 7 - Designazione Sub-Responsabili (Sub-Fornitori)

7.1. – Il Responsabile del trattamento non designerà alcun Sub-Responsabile in relazione a qualsiasi trattamento dei dati personali, senza previa autorizzazione scritta del Titolare. Il Responsabile è tenuto, pertanto, a presentare la richiesta di autorizzazione specifica, di cui all'Allegato B, almeno 30 giorni prima di ricorrere al Sub-Responsabile, unitamente alle informazioni necessarie per consentire al Titolare del trattamento di decidere in merito all'autorizzazione.

7.2. Il Titolare si riserva la facoltà di opposizione alla richiesta di autorizzazione/modifica del Sub-Responsabile. Tale opposizione dovrà essere notificata al Responsabile attraverso un atto scritto all'interno del quale il Titolare è tenuto ad esprimere le ragioni della propria opposizione.

In caso di mancato riscontro da parte del Titolare entro il termine di cui al precedente punto 7.1, il Responsabile acquista l'autorizzazione alla nomina/modifica del Sub—Responsabile

7.3. Il Responsabile è tenuto, altresì, a comunicare ogni eventuale modifica e/o sostituzione riguardante i Sub-Responsabili approvati, le quali dovranno essere a loro volta approvate dal Titolare.

7.4. Il Responsabile:

- si impegna a selezionare Sub-Responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti e risponda alle esigenze del GDPR e garantisca la tutela dei diritti degli interessati.
- limiterà l'accesso del Sub-Responsabile ai dati personali necessari per soddisfare gli obblighi del Responsabile ai sensi della nomina. Al Sub-Responsabile sarà vietato l'accesso ai dati personali per qualsiasi altro scopo;
- imporrà per iscritto ad ogni Sub-Responsabile il rispetto di obbligazioni e istruzioni equipollenti a quelle previste nel presente ATTO di nomina nella sua totalità.
- rimarrà pienamente responsabile nei confronti del Titolare per il rispetto degli obblighi derivanti dal presente ATTO di nomina per qualsiasi atto o omissione del Sub-Responsabile che comporti una violazione degli stessi."

Articolo 8 – Trasferimento dati verso paesi terzi e/o organizzazioni internazionali

8.1. Le Parti si danno reciprocamente atto che il trasferimento dei dati personali oggetto del presente ATTO non avverrà, di regola, al di fuori dello SEE.

8.2. Nel caso in cui, in ragione dell'esecuzione dell'Accordo, il Titolare autorizzi il Responsabile (o il Sub-Responsabile) a trasferire i dati personali verso Paesi terzi e/o organizzazioni internazionali, il

Responsabile del trattamento si impegna ad effettuare tale trasferimento dei dati soltanto previa istruzione documentata del Titolare e secondo uno dei meccanismi previsti dal GDPR.

Articolo 9 – Inosservanza e risoluzione

Qualora il Responsabile del trattamento violi gli obblighi di cui all'Accordo e/o al presente ATTO, il Titolare, in base all'entità della violazione, può dare istruzione al Responsabile di sospendere il trattamento dei dati personali, concedendo un termine di sospensione pari a giorni 30 (trenta) entro il quale il Responsabile dovrà adempiere agli obblighi di cui sopra.

Nel caso in cui il Responsabile non si adegui alle prescrizioni dell'Accordo e/o del presente ATTO e non dimostri di poterle rispettare entro il termine di sospensione, il Titolare potrà risolvere di diritto l'Accordo e l'ATTO.

In ogni caso, il Titolare del trattamento può risolvere di diritto il presente ATTO, con conseguente risoluzione dell'Accordo, nel caso in cui:

Il Responsabile violi in modo sostanziale e/o persistente gli obblighi che gli incombono a norma della vigente normativa in ambito privacy e del presente ATTO;

Il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente o della Autorità di controllo competente per quanto riguarda i suoi obblighi in conformità alle presenti clausole o del Regolamento UE 2016/679 e/o del Regolamento UE 2018/1725.

Il Responsabile del trattamento può risolvere di diritto il presente ATTO, con conseguente risoluzione dell'Accordo, nel caso in cui:

Dopo aver informato il Titolare che le sue istruzioni violano la vigente normativa in ambito privacy, il Titolare insista sul rispetto delle stesse.

Articolo 10 – Responsabilità

Ferma restando la previsione di cui all'art. 82 GDPR, ciascuna parte si impegna a tenere indenne l'altra parte da qualsiasi pretesa fatta valere da terzi a causa di e/o in relazione a qualsiasi violazione colposa e/o dolosa commessa.

Articolo 11 – Comunicazioni

Tutte le comunicazioni tra le Parti, ai sensi del presente ATTO, saranno fatte per iscritto e verranno considerate validamente effettuate se inviate a mezzo PEC, lettera raccomandata a/r e/o e-mail, ai seguenti indirizzi:

TITOLARE:

Regione Basilicata

Direttore Generale della Direzione Generale per la Salute e le Politiche della Persona

Viale Vincenzo Verrastro, 9 Potenza

P.E.C.:

RESPONSABILE:

P.E.C.: _____

Letto, approvato e sottoscritto

_____, lì _____

Il Titolare

Il Responsabile

Allegato A

Modulo Segnalazione Evento Data Breach

SINTETICA DESCRIZIONE DELLA VIOLAZIONE (ES: INVIO ERRATO DI E.MAIL)	
Data violazione	
Orario in cui ci si è accorti della violazione	
Luogo della violazione (in caso di smarrimento di dispositivi portatili)	
Cause della violazione	
Tipologia della violazione	ES: perdita di riservatezza, disponibilità, integrità/esattezza
Informazioni, dati e numero dei dati oggetto della violazione	
Categorie di Interessati coinvolti	
Fonte della segnalazione	(se siete venuti a conoscenza indirettamente della violazione, indicare chi ve lo ha segnalato e come)
Descrizione dell'evento	(in modo più accurato possibile)
Misure adottate a seguito della scoperta della violazione	
Descrizione delle probabili conseguenze della violazione dei dati personali	

Allegato B

Richiesta di autorizzazione a nominare un sub-responsabile

Il Fornitore da voi nominato Responsabile del trattamento in virtù dell'Accordo di servizi del _____, con la presente richiede la possibilità di nominare un Sub-Responsabile al trattamento al fine di poter assolvere le attività da voi affidate, nel modo più idoneo e coerente con il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR) e della normativa italiana di recepimento e di adeguamento.

In particolare il Sub Responsabile del trattamento sarà individuato nella Società/nella persona di _____, altamente specializzato/a in _____, cui il Responsabile affiderà l'attività di _____ necessaria a _____.

Restando in attesa di un Vostro cortese riscontro, porgiamo i nostri più cordiali saluti.

Data ____/____/____

Il Responsabile
