

AFFIDAMENTO DI UN SERVIZIO DI SVILUPPO, PERSONALIZZAZIONE E DIFFUSIONE DEL SISTEMA SOFTWARE A SUPPORTO DELLE COT E RELATIVO SUPPORTO SPECIALISTICO.

M6C1 I1.2.2 – Centrali operative territoriali (COT)– Interconnessione aziendale

Procedura negoziata senza previa pubblicazione di bando nel caso di fornitura/servizi ritenuti infungibili ai sensi
dell'art. 76 co. 2 lett. b del **D.lgs. 36/2023**

CIG -**XXXXXXX**

SCHEMA DELL'ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

CUP D27H22000970006

[Da valutare se valorizzare diversamente i riferimenti al Titolare, al Responsabile, al sub Responsabile, ai terzi autorizzati al Trattamento. In caso di R.T.I., occorre verificare se tutte le società del R.T.I. effettuino il trattamento di dati personali, in tal caso può essere inserita la seguente clausola nel contratto; in caso contrario, si potrebbe non inserire la seguente clausola per procedere con separati atti di nomina delle sole società che effettuano il trattamento di dati personali, utilizzando il contenuto della clausola]

Con la sottoscrizione della presente da parte di **Azienda Regionale della Salute – ARES Sardegna** (nel prosieguo l'«**Amministrazione**», o «**Titolare del Trattamento**»), il Fornitore [...] è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 (di seguito anche il «**Responsabile del Trattamento**» o il «**Responsabile Iniziale**») sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche «**Regolamento UE**»), per tutta la durata del contratto esecutivo (nel seguito anche «**Contratto Esecutivo**») relativo all'affidamento di SERVIZIO DI SVILUPPO, PERSONALIZZAZIONE E DIFFUSIONE DEL SISTEMA SOFTWARE A SUPPORTO DELLE COT E RELATIVO SUPPORTO SPECIALISTICO. A tal fine, il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto dell'Amministrazione, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del Contratto Esecutivo, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE, del D.Lgs. n. 196/2003 e s.m.i. e del D.Lgs. n. 101/2018 (nel seguito anche «**Normativa in tema di trattamento dei dati personali**»), e delle istruzioni nel seguito fornite.

1. Il Fornitore si impegna a presentare su richiesta dell'Amministrazione garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile Iniziale.
2. Le finalità del trattamento sono consistono nella necessità di garantire l'esecuzione, da parte del Fornitore, del Contratto Esecutivo con l'Amministrazione [Valutare l'inserimento di ulteriori finalità giustificative del trattamento dei dati].
3. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati personali comuni; ii) dati appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento UE; iii) dati relativi a condanne penali e reati ai sensi dell'art. 10 del Regolamento UE. [Valutare l'inserimento di ulteriori categorie di dati personali].
4. Le categorie di interessati comprendono tutti i soggetti assistiti dal sistema sanitario di Regione Sardegna [Valutare l'inserimento di ulteriori categorie di soggetti interessati in ragione dell'oggetto del Contratto Esecutivo: es. dipendenti e collaboratori, altri utenti dei servizi, ecc.].
5. Nell'esercizio delle proprie funzioni, il Responsabile del Trattamento si impegna a:
 - a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del Contratto Esecutivo;
 - b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

- c) trattare i dati personali conformemente alle istruzioni impartite dal Titolare del Trattamento e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del contratto (d'ora in poi «**Persone Autorizzate**»); nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del Trattamento;
- d) garantire la riservatezza dei dati personali trattati nell'ambito del contratto e verificare che le Persone Autorizzate a trattare i dati personali in virtù del contratto:
 - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
 - ricevano la formazione necessaria in materia di protezione dei dati personali;
 - trattino i dati personali osservando le istruzioni impartite dal Titolare del Trattamento al Responsabile del Trattamento;
- e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (*privacy by default*);
- f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, 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 illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
- g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;
- h) [\[Tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato o includa il trattamento di dati sensibili di cui all'articolo 9, paragrafo 1, o i dati giudiziari di cui all'articolo 10\]](#), ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare del Trattamento e dell'Autorità, laddove ne venga fatta richiesta;
- i) adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla Circolare AgID n. 2/2017 del 18 aprile 2017 [\[Specificare il livello richiesto tra quelli previsti nella Circolare\]](#).

6. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore si impegna a fornire

all'Amministrazione un piano di misure di sicurezza rimesse all'approvazione della stessa, che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso [\[personalizzare in ragione dell'oggetto del Contratto Esecutivo\]](#):

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- d) una procedura 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.

7. Il Responsabile del trattamento deve mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

A tal fine, il Titolare informa preventivamente il Responsabile del Trattamento con un preavviso minimo di tre [\[o diverso termine indicato dalla PA\]](#) giorni lavorativi; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento UE, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà le penali previste e diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c., l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

[\[ARES deve selezionare una delle due ipotesi indicate nei capoversi precedenti e identificate con i numeri "1\)" e "2\)"\]](#)

8. [1\) \[Autorizzazione generale\]](#) Il Responsabile del Trattamento può ricorrere ad un altro Responsabile del Trattamento (di seguito, il «**Sub-Responsabile del Trattamento**») per gestire attività di trattamento specifiche, informando, periodicamente [...] [\[La PA deve specificare la periodicità\]](#), il Titolare del Trattamento delle nomine e delle sostituzioni dei Responsabili del Trattamento. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei Sub-Responsabili del Trattamento nominati e i dati del contratto di esternalizzazione.

[Oppure]

2) [Autorizzazione specifica] Il Responsabile del Trattamento può avvalersi di un ulteriore Responsabile del Trattamento (di seguito, il «**Sub-Responsabile del Trattamento**») per delegargli attività specifiche, previa autorizzazione scritta del Titolare del Trattamento.

9. Il Sub-Responsabile del Trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale, riportate 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; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del Sub-Responsabile del Trattamento, tramite *audit* e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile Iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e *audit* le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento UE o risulti che il Sub-Responsabile del Trattamento agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà al Responsabile Iniziale del trattamento le penali e diffiderà lo stesso a far adottare al Sub-Responsabile del Trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 c.c., l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il Contratto Esecutivo con il Responsabile Iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

10. Il Responsabile del Trattamento deve assistere il Titolare del Trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto [selezionare una tra le due opzioni indicate nei capoversi seguenti e identificate con i numeri "1)" e "2)"]:

1) ad informare tempestivamente il Titolare del Trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del Trattamento, nei termini previsti dalla Regolamento UE; oppure

2) ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti].

Il Responsabile del Trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare del Trattamento di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del Trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare del Trattamento ne viene a conoscenza;

nel caso in cui il Titolare del Trattamento debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del Trattamento [da valorizzare in alternativa: Sub-Responsabile del Trattamento] si impegna a supportare il Titolare del Trattamento nell'ambito di tale attività.

11. Il Responsabile del Trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare del Trattamento in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare del Trattamento nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del Contratto Esecutivo.
12. Il Responsabile del Trattamento deve comunicare al Titolare del Trattamento il nome ed i dati del proprio soggetto responsabile della protezione dei dati, qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE (di seguito il «**Soggetto Responsabile della protezione dei dati**»); il Soggetto Responsabile della protezione dei dati del Responsabile del Trattamento collabora e si tiene in costante contatto con il Soggetto Responsabile della protezione dei dati del Titolare del Trattamento.
13. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile del Trattamento, su richiesta del Titolare, si impegna a:
 - a) restituire al Titolare del Trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati;
 - b) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
14. Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine, secondo quanto previsto dal Provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
15. Il Responsabile del Trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i dati personali, trattati nell'espletamento del Contratto Esecutivo, siano precisi, corretti e aggiornati nel corso della durata del trattamento – anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati – eseguito dal Responsabile del Trattamento, o da un Sub-Responsabile del Trattamento.
16. Il Responsabile del Trattamento 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 del Trattamento.
17. Sarà obbligo del Titolare del Trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del Trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.
18. Durante l'esecuzione del Contratto Esecutivo, nell'eventualità di qualsivoglia modifica della Normativa in tema di trattamento dei dati personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del Trattamento si impegna a

collaborare – nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse – con il Titolare del Trattamento affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

19. Il Responsabile del Trattamento manleverà e terrà indenne il Titolare del Trattamento da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della Normativa in tema di protezione dei dati personali e/o della disciplina sulla protezione dei dati personali comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori.
20. [\[Da valutare l'opportunità di inserire un rinvio alle eventuali ulteriori previsioni contenute nel capitolato tecnico in relazione al tema della protezione dei dati personali\].](#)