Allegato 1 – Schema di Contratto

DATA PROCESSING AGREEMENT

(art 28 del Regolamento UE 679/2016 - GDPR)

Procedura aperta da espletarsi mediante utilizzo della Piattaforma Telematica SardegnaCAT, ai sensi degli articoli 58 e 60 del D. Lgs. n. 50/2016 per l'appalto triennale del servizio di supporto ai servizi assistenziali nei plessi ospedalieri delle "Cliniche di San Pietro" e del "SS Annunziata" dell'Azienda Ospedaliero Universitaria di Sassari. Importo complessivo triennale a base di gara, € 23.412.158,32 (di cui € 1.750,00 per oneri per la sicurezza, non soggetti a ribasso), oltre IVA nella misura di legge, ripetibile per due annualità, per un importo complessivo dell'investimento, incluse tutte le ripetizioni programmate opzionabili ed eventuali modifiche contrattuali, di € 50.725.468,03 (IVA esclusa). N°. gara ANAC 8059481 - CIG 8641761EC3. CUI S02268260904202000013 – CPV 85110000-3.85110000-3.

Criterio di aggiudicazione

OEPV, sulla base del miglior rapporto qualità prezzo

(95, comma 2, del D. Lgs. n. 50/2016)

Il Contraente è nominato dal Titolare (A.O.U. di Sassari), ai sensi dell'art 28 del Regolamento UE 679/2016 (GDPR) Responsabile delle operazioni di trattamento dei dati personali previste per l'esecuzione del contratto principale in essere tra le parti, definendo gli obblighi delle medesime parti in materia di tutela dei dati personali.

Il Contraente si impegna, pertanto, a sottoscrivere il presente "Data Processing Agreement", che costituisce parte integrante e sostanziale del contratto.

1. Natura e finalità del trattamento

Il Responsabile tratta i dati personali nella misura strettamente necessaria all'esecuzione del contratto principale e per le finalità individuate da quest'ultimo.
Il Titolare fornisce, di seguito, al Responsabile le pertinenti istruzioni cui attenersi nello svolgimento dell'incarico. Esse integrano quanto eventualmente già specificato nel contratto principale.

2. Obblighi del responsabile del trattamento

Il Responsabile – per quanto di propria competenza – è tenuto, in forza di legge e di contratto, al rispetto della riservatezza, integrità e qualità dei dati ed a utilizzarli esclusivamente per le finalità specificate e nell'ambito delle attività connesse all'esecuzione del Contratto.

Il Responsabile esterno del trattamento può autonomamente assumere decisioni in ambito tecnico ed organizzativo con riguardo al servizio che sta offrendo; in nessun caso potrà variare le finalità e modalità del trattamento definite dal Titolare, ne potrà usare i dati per propri scopi.

Nel caso in cui il Responsabile esterno decida di usare i dati per scopi propri ovvero per finalità o tramite mezzi non corrispondenti a quanto definito dal Titolare, sarà considerato a sua volta un Titolare per le attività di trattamento per le quali ha definito le finalità e/o i mezzi in autonomia, fatta salva la sua responsabilità per l'utilizzo illecito dei dati.

Il Responsabile esterno deve garantire che le persone da lui autorizzate al trattamento dei dati personali abbiano un adeguato obbligo legale alla riservatezza ed un'adeguata formazione in materia di protezione dei dati personali.

3. Misure di sicurezza dei dati trattati

Il Responsabile esterno del trattamento ha l'obbligo di individuare ed adottare adeguate misure tecniche ed organizzative idonee a garantire la sicurezza dei dati trattati per conto del Titolare. Le misure dovranno essere commisurate al rischio per i diritti e le libertà degli interessati, dovranno soddisfare i requisiti di cui all'articolo 32 del GDPR e potranno comprendere, tra le altre, se del caso:

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 di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, il Responsabile tiene conto, in particolare, dei rischi connessi al trattamento che possono derivare dalla perdita, dalla distruzione, dalla modifica, dalla diffusione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

4. Compiti del responsabile del trattamento

Il Responsabile esterno del trattamento dovrà porre in essere le seguenti attività legate al suo ruolo, salvo le ulteriori nascenti dal rispetto del GDPR o della normativa nazionale in corso di emanazione da parte del Governo, relativamente ai trattamenti che discendono dall'esecuzione del contratto principale, come da prospetto:

- lo svolgimento di attività di trattamento dati per conto del Titolare nella misura strettamente necessaria all'esecuzione del contratto principale (articolo 28, paragrafo 3 lettera a, del GDPR);
- la garanzia che i trattamenti eseguiti in esecuzione del contratto principale siano effettuati nel rispetto dei principi di liceità, correttezza, trasparenza e finalità, nonché nel rispetto delle garanzie previste dal Regolamento (articoli 5 – 9 del GDPR);
- la possibilità di delegare - come sub Responsabili del trattamento – altri soggetti per l'esecuzione di specifiche attività che discendano direttamente dal contratto principale, previa comunicazione scritta al Titolare del trattamento e dietro sua autorizzazione specifica (articolo 28, paragrafo 2, del GDPR). Il Fornitore/Responsabile rimane responsabile nei confronti dell'AOU Sassari per l'adempimento del sub Responsabile agli obblighi discendenti dal GDPR e dal presente accordo;
- la redazione e la tenuta di un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare - Registro dei trattamenti del Responsabile (articolo 30, paragrafo 2, del GDPR) contenente:
    a) il nome e i dati di contatto del Responsabile, del Titolare e degli eventuali sub Responsabili;
    b) le categorie dei trattamenti effettuati per conto del Titolare del trattamento;
    c) eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
    d) una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

- la periodica valutazione dell'impatto delle procedure e dell'organizzazione sulla tutela dei dati personali - DPIA (articolo 35 del GDPR);
- l'individuazione delle misure ritenute necessarie per garantire adeguati livelli di protezione dei dati trattati e l'adeguamento tempestivo alle stesse (articolo 32 del GDPR);
- la collaborazione con il Titolare del Trattamento e con il Responsabile della Protezione Dati nominato per l'adempimento degli obblighi derivanti dall'applicazione del GDPR e per l'attuazione delle prescrizioni impartite dal Garante;
- la collaborazione nella gestione del Data Breach, con l'obbligo per il Responsabile del trattamento di informare il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione, al fine di permettere al Titolare di rispettare il termine di notifica al Garante previsto dall'articolo 33 del GDPR;
- l'individuazione - all'interno della propria organizzazione - dei soggetti autorizzati a compiere attività di trattamento, la loro nomina formale, la comunicazione al Titolare dell'avvenuta nomina ed il compito di fornire ai soggetti autorizzati indicazioni puntuali sulla modalità di espletamento dei compiti assegnati.

5. Istanze degli interessati

Nel caso in cui il Responsabile riceva istanza dagli interessati per l'esercizio dei diritti loro attribuiti dagli articoli dal 12 al 23 del GDPR, il Fornitore deve provvedere a:

- darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta;
- informare l'interessato dell'avvenuta trasmissione degli atti al Titolare, cui competerà rispondere direttamente;
- assistere la AOU Sassari per la soddisfazione delle richieste degli interessati senza ritardo e comunque nel rispetto del termine ultimo previsto dal GDPR;
- coordinarsi a tal fine con il Titolare, con il Servizio Affari Generali, Comunicazione e Rapporti con l'Università - in qualità di soggetto preposto dal Titolare alle relazioni con i soggetti interessati - e con il Responsabile della Protezione Dati.

6. Verifiche del titolare

Il Responsabile si impegna a mettere a disposizione della AOU Sassari tutte le informazioni necessarie a dimostrare il rispetto degli obblighi tipici dei Responsabili del trattamento di cui all'articolo 28 del GDPR.

Il Responsabile riconosce al Titolare il diritto di effettuare o far effettuare, prima, durante o dopo le operazioni di trattamento, verifiche finalizzate ad accertare il rispetto delle istruzioni fornite e il conforme svolgimento del trattamento. L'intenzione da parte dell'AOU Sassari di svolgere o far svolgere verifiche, ispezioni o audit dovrà essere comunicata al Fornitore con congruo anticipo e comunque con almeno 10 giorni di preavviso.

7. Scadenza del contratto

Il Responsabile si impegna a interrompere qualsiasi forma di trattamento dati effettuati per conto del Titolare alla scadenza del contratto o del diverso termine eventualmente dallo stesso previsto.

A discrezione dell'AOU Sassari, tutti i dati personali trattati dal Responsabile per conto del Titolare, devono essere restituiti a quest'ultimo e/o cancellati, salvo che la legge applicabile imponga al Fornitore la conservazione per un periodo ulteriore dei dati personali trattati.

Se le Operazioni di Trattamento si svolgono presso il Titolare su apparati nella disponibilità di quest'ultimo, sui quali siano state fornite al Responsabile e ai suoi incaricati le necessarie autorizzazioni e credenziali di autenticazione, all'atto della cessazione delle Operazioni di Trattamento le autorizzazioni vengono revocate e le credenziali disattivate.

Sassari, lì _____

Per l'Azienda Ospedaliero Universitaria di Sassari
Il Rappresentante Legale

_____

Per l'Operatore Economico Concorrente
Il Rappresentante Legale

_____