



## **ACCORDO PER LA NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI** (ex articolo 28 del Regolamento UE 679/2016)

**tra**

L'AOU di Sassari, con sede legale in Viale S.Pietro, 10 – 07100 Sassari P. IVA 02268260904 rappresentata dal Rappresentante legale p.t. del Titolare del Trattamento (in seguito detto il TITOLARE del trattamento)

**e**

Federfarma Sardegna - Unione Sindacali e dei titolari di Farmacia - Regione Sardegna (qui di seguito definita "Federfarma"), con sede in Cagliari, via Biasi 25, rappresentata dal Presidente Dott. Giorgio Congiu, domiciliato, per la carica ricoperta, presso la sede di Federfarma Sardegna (in seguito detta il RESPONSABILE del trattamento);

**VISTI**

- il Regolamento UE 679/2016 del Parlamento e della Commissione 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);
- la Convenzione n. 6/2020 prot. n. 14272 del 16.06.2020 tra Regione Autonoma della Sardegna (RAS) e Federfarma per l'erogazione di servizi ICT presso le farmacie convenzionate;
- la Convenzione attuativa tra l'Azienda Ospedaliero Universitaria di Sassari e Federfarma Sardegna, di cui alla Delibera n. \_\_\_\_\_ del \_\_\_\_\_

**DATO ATTO**

- che a norma dell'articolo 32 del GDPR è compito del Titolare individuare e predisporre le idonee misure organizzative e tecniche che offrano adeguati livelli di sicurezza del dato, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento;
- che per l'esecuzione del servizio oggetto della convenzione il Responsabile del trattamento svolgerà per conto dell'Azienda Ospedaliero Universitaria di Sassari operazioni di trattamento di dati personali così come definite dall'articolo 4 del GDPR, connessi alle seguenti finalità:
  - attivazione delle TS-CNS e rilascio del certificato di firma digitale;
  - diffusione, apertura ed utilizzo del FSE;
  - scelta e revoca online del medico;



- prenotazione delle prestazioni sanitarie;
- pagamento del ticket online.
- che il Responsabile del trattamento gode di competenze e conoscenze tecniche ed organizzative in relazione alle modalità delle operazioni, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati trattati, nonché alla normativa in materia di tutela dei dati personali;
- che per l'erogazione dei servizi in oggetto il Responsabile si avvale della procedura informatizzata per la registrazione del consenso secondo le modalità fornite dalla Regione per il tramite di Sardegna IT;
- che l'AOU Sassari svolge il ruolo di Titolare del trattamento dei dati personali da essa operato, in quanto decide autonomamente sulle finalità e modalità dello stesso;
- che il Titolare intende nominare il fornitore del servizio – che intende accettare tale nomina – quale Responsabile delle operazioni di trattamento oggetto della presente convenzione;
- che le Parti, in relazione a tale nomina, intendono regolare con il presente accordo i loro reciproci rapporti in tema di disciplina dei trattamenti dei dati personali effettuati dal Responsabile per conto di Titolare;
- che a norma dell'articolo 82 del GDPR qualsiasi danno causato da una violazione del Regolamento è risarcibile e che la responsabilità tra Titolare e Responsabile del trattamento è solidale;

**TUTTO CIO PREMESSO**

**LA AOU SASSARI**

**E**

**FEDERFARMA**

stipulano il seguente accordo per la nomina a Responsabile esterno del Trattamento dei Dati Personali (in seguito detto anche RESPONSABILE del TRATTAMENTO).

**Art.1**

**Ambito di applicazione**

- Il presente accordo è lo strumento che l'AOU di Sassari adotta al fine di disciplinare in maniera conforme al Regolamento UE 679/2016, (c.d. GDPR) le operazioni di trattamento dati previste nell'ambito dell'esecuzione dei servizi di cui alla convenzione da parte delle farmacie convenzionate;
- Il presente accordo stabilisce l'obbligo - che s'instaura tra l'AOU di Sassari, Federfarma e le farmacie convenzionate - d'improntare le proprie misure sicurezza e di tutela nel trattamento dati ai principi del Regolamento UE 679/2016;
- Il presente accordo costituisce parte integrante della convenzione per l'erogazione di servizi ICT presso le farmacie convenzionate in essere tra le parti;



- Per quanto non disciplinato dal presente accordo si rinvia al Regolamento UE 679/2016, al rispetto del quale sono tenuti i dipendenti d'impresе fornitrici di beni o servizi e che realizzano opere in favore dell'Amministrazione.

## **Art.2**

### **Oggetto**

Con il presente accordo, ai sensi dell'articolo 28 del GDPR, il TITOLARE nomina Federfarma in qualità di Responsabile esterno delle operazioni di Trattamento dei Dati Personali previste per l'esecuzione del contratto principale in essere tra le parti e vengono definiti gli obblighi delle medesime parti in materia di tutela dei dati personali.

## **Art. 3**

### **Natura e finalità del trattamento**

Il Responsabile del trattamento 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 del TRATTAMENTO le pertinenti istruzioni cui attenersi nello svolgimento dell'incarico. Esse integrano quanto eventualmente già specificato nel contratto principale.

## **Art. 4**

### **Obblighi del Responsabile del Trattamento**

Il RESPONSABILE del TRATTAMENTO – 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 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 del TRATTAMENTO decida, indebitamente, 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 le sue responsabilità per la sottrazione e l'utilizzo illecito dei dati.

Sarà cura del RESPONSABILE del TRATTAMENTO designare, nell'ambito della propria organizzazione, i dipendenti incaricati del trattamento, fornire loro istruzioni, sovrintendere e vigilare sull'attuazione delle istruzioni impartite, inviare la lista degli incaricati al Titolare e mantenerla aggiornata.



Il RESPONSABILE del TRATTAMENTO deve garantire che, nell'ambito della propria organizzazione, i dipendenti da lui autorizzati al trattamento dei dati personali, abbiano un adeguato obbligo legale alla riservatezza ed un'adeguata formazione in materia di protezione dei dati personali.

### **Art. 5**

#### **Misure di sicurezza**

Il RESPONSABILE 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.

Nel valutare l'adeguato livello di sicurezza, il RESPONSABILE del TRATTAMENTO 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.

### **Art. 6**

#### **Compiti del Responsabile del Trattamento**

Il RESPONSABILE del TRATTAMENTO dovrà porre in essere le seguenti attività legate al suo ruolo, salvo le ulteriori nascenti dal rispetto del GDPR e/o della normativa nazionale di coordinamento, 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 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 medesimo di rispettare il termine di notifica al Garante previsto dall'articolo 33 del GDPR;
  - la nomina del personale in qualità di soggetti autorizzati a compiere attività di trattamento, la comunicazione al TITOLARE dell'avvenuta nomina ed il compito di fornire ai soggetti autorizzati indicazioni puntuali sulla modalità di espletamento dei compiti assegnati.

#### **Art. 7**

##### **Istanze degli interessati**

Nel caso in cui il RESPONSABILE del TRATTAMENTO 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.

#### **Art. 8**

##### **Verifiche del Titolare**

Il FORNITORE 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 del TRATTAMENTO 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.

### **Art. 9**

#### **Scadenza del contratto**

Il RESPONSABILE del TRATTAMENTO 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 per conto del TITOLARE, devono essere restituiti a quest'ultimo e/o cancellati/distrutti, salvo che la legge applicabile gli imponga la conservazione per un periodo ulteriore dei dati personali trattati.

All'atto della cessazione delle Operazioni di Trattamento le autorizzazioni vengono revocate e le credenziali sul sistema informatico fornito da Sardegna IT vanno disattivate.

### **Art. 10**

#### **Variazioni**

Il contenuto del presente documento potrà essere integrato dall'AOU di Sassari da eventuali futuri protocolli.

Federfarma dichiara di aver letto e di accettare espressamente, tutte le disposizioni contenute negli articoli della presente scrittura.

Luogo e data \_\_\_\_\_

Il Commissario Straordinario f.f.

Il Rapp.te legale di Federfarma Sardegna

\_\_\_\_\_

\_\_\_\_\_