Accordo per la designazione del Responsabile del Trattamento dei dati personali ed adempimenti correlati ai sensi del Regolamento Europeo sulla protezione dei dati personali 2016/679.

Premesso che:

con Contratto per _____ CIG _____ (di seguito "Contratto"), la società _____, con sede in _____, P.IVA _____ (di seguito il "Fornitore" o il "Responsabile"), si impegna a fornire ad AIFA, con sede in via del Tritone 181, Roma (di seguito "AIFA" o il "Titolare"), servizi che prevedono il trattamento di dati personali di titolarità di quest'ultima;

il Fornitore dichiara di essersi conformato al Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ed alle altre norme applicabili in materia di protezione dei dati personali (di seguito "GDPR" o "Regolamento");

il Fornitore dichiara di essere dotato dell'esperienza, dell'affidabilità e delle capacità necessarie per l'espletamento della funzione di responsabile del trattamento di cui all'articolo 28 del Regolamento;

il Fornitore dichiara e garantisce, sin d'ora, di godere di competenza e conoscenze tecniche in relazione alle finalità e modalità del trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati trattati nonché di un livello di sicurezza adeguato al rischio;

il presente Accordo annulla e sostituisce ogni altro atto precedente accordo, scritto e/o orale, intercorso tra le Parti in relazione alla nomina di responsabile esterno del trattamento.

Tutto ciò premesso AIFA, in qualità di Titolare del Trattamento, designa con il presente Atto, ai sensi dell'art. 28 del GDPR, il Fornitore quale

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Il Fornitore, con la sottoscrizione del presente Accordo, dichiara espressamente di accettare la designazione e di conoscere gli obblighi che, per effetto di tale accettazione, si impegna ad assumere in relazione a quanto prescritto dal Regolamento, da ogni altra normativa applicabile in materia di protezione dei dati personali nonché dal presente Accordo, disciplinato dai seguenti termini e condizioni.

1. Oggetto

Le Parti si impegnano a rispettare la Normativa Privacy vigente in relazione alla determinazione delle finalità e modalità del trattamento di dati personali nell'ambito delle attività previste dal Contratto o a questo comunque connesse (di seguito i "**Servizi**").
Con riferimento al trattamento dei dati personali nell'ambito dei Servizi, AIFA, Titolare del trattamento, accetta che il Fornitore, nel rispetto dell'art. 28 GDPR, tratti per suo conto i dati personali in qualità di Responsabile del trattamento (il "**Responsabile**").

Il Responsabile tratterà i dati personali inerenti i servizi e/o le forniture oggetto del Contratto per le relative finalità.

2. Impegni del Responsabile:

Il Fornitore si impegna a:

- effettuare esclusivamente i trattamenti connessi alle operazioni affidategli sulla base delle istruzioni del Titolare e comunque nell'esecuzione del Contratto, con divieto di qualsiasi altra diversa utilizzazione e con espresso divieto di estrarne copia, parziale o totale, salvo eventuali trattamenti obbligatori in base alla Normativa Privacy;
- individuare le persone autorizzate al trattamento e provvedere alla formalizzazione della relativa designazione, corredata da adeguate istruzioni, con particolare riguardo alle misure di sicurezza, vigilando sul loro operato e sulla corretta applicazione delle istruzioni impartite, prescrivendo altresì che le stesse abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- far sì che tutti i suoi dipendenti e/o collaboratori, inclusi gli eventuali subappaltatori, autorizzati a trattare i dati personali del Titolare, siano soggetti ad obblighi di confidenzialità;
- far sì che tutti i suoi dipendenti e/o collaboratori, inclusi i subappaltatori, autorizzati a trattare i dati del Titolare, abbiano seguito attività di formazione sulle normative in materia di trattamento dei dati personali, abbiano ricevuto, relativamente ai trattamenti effettuati, istruzioni specifiche che siano coerenti con le istruzioni impartite al Responsabile dal Titolare e proteggano – infine – i dati personali in maniera tale da minimizzare il rischio di distruzione, perdita, anche accidentale, dei dati medesimi, e di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- individuare gli amministratori di sistema e designarli rispettando i requisiti previsti dal provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 settembre 2008 ("Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"), così come modificato il 25 giugno 2009;
- periodicamente verificare, con cadenza almeno annuale, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione dei soggetti autorizzati al trattamento, compresi gli amministratori di sistema;
- adottare, prima dell'inizio del trattamento, adeguate misure di sicurezza atte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali, di accessi non autorizzati o di trattamenti non consentiti o non conformi, nel rispetto dell'Articolo 32 del GDPR, tenuto conto dello stato dell'arte e del progresso tecnico, nonché dei rischi connessi ai dati personali oggetto di trattamento. Queste misure includono, tra le altre, se del caso: (i) la pseudonimizzazione e la cifratura dei dati personali; (ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; (iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; (iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- avvisare tempestivamente il Titolare in caso di richieste ricevute dagli interessati quali forme di esercizio dei diritti di cui al capitolo III del GDPR. Inoltre, tenuto conto della natura del Trattamento di volta in volta effettuato, anche nel caso in cui il Titolare sia in possesso di tutte le informazioni per rispondere autonomamente, il Responsabile fornirà la ragionevole

assistenza al Titolare, per quanto possibile, per l'adempimento dell'obbligo di quest'ultimo di rispondere alle richieste degli interessati;

- avvisare tempestivamente il Titolare di ogni eventuale ispezione, controllo, richiesta provenienti dal Garante per la protezione dei dati personali, dall'Autorità Giudiziaria o da qualsiasi ulteriore Autorità competente in relazione ai Servizi di cui al Contratto, collaborando con il Titolare nel riscontro e/o esecuzione di tali attività;
- tenuto conto della natura del Trattamento e delle informazioni disponibili, fornire assistenza al Titolare, sulla base di quanto di volta in volta concordato, in relazione a quanto segue:
  a. obblighi del Titolare di notificare alle Autorità di vigilanza e ai soggetti interessati le violazioni dei Dati Personali di cui agli artt. 33 e 34 del GDPR;
  b. obblighi del Titolare in materia di valutazione di impatto sulla protezione dei dati di cui all'articolo 35 del GDPR;
  c. obblighi del Titolare relativi alla consultazione preventiva di cui all'articolo 36 del GDPR;
- durante le attività di monitoraggio e controllo del Titolare, mettere a disposizione tutte le informazioni richieste, assicurando al Titolare e/o ai soggetti da questi di volta in volta incaricati la possibilità di effettuare adeguate verifiche sul trattamento dei dati;
- informare immediatamente il Titolare qualora, a parere del Responsabile, un'istruzione ricevuta dal Titolare violi la Normativa Privacy.

3. Divieto di cessione del contratto e disciplina del Sub-responsabile.

3.1. Il presente Accordo non può essere oggetto di cessione a terzi.
Il Responsabile potrà avvalersi di un altro responsabile del trattamento ("**Sub-responsabile**") per l'esecuzione di specifiche attività di trattamento per conto del Titolare:

a. previa autorizzazione del Titolare, secondo le modalità stabilite all'articolo 3.2;
b. a condizione che il contratto con il Sub-Responsabile sia stipulato per iscritto, preveda a carico del Sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nel presente Accordo, ed assicuri il rispetto dei requisiti previsti dall'art. 28 GDPT, tra cui – in particolare – la previsione di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti delle normative in materia di privacy;
c. a condizione che il contratto con il Sub-responsabile cessi automaticamente di avere effetto allo spirare del Contratto tra le Parti, per qualsiasi ragione.

3.2 Il Responsabile dovrà preventivamente comunicare per iscritto al Titolare l'intenzione di avvalersi di un Sub-responsabile (compresa la sua sostituzione). In tale comunicazione, il Responsabile fornirà tutti i dettagli utili, incluse le attività di trattamento che intende trasferire al Sub-responsabile, perché le effettui in luogo del Responsabile, affinché il Titolare possa valutarne l'idoneità. Qualora, entro 10 giorni lavorativi dalla ricezione della comunicazione, il Titolare comunichi per iscritto al Responsabile la propria opposizione alla designazione proposta, il Responsabile non potrà nominare il Sub-responsabile proposto.

3.3. Con riferimento a qualsiasi Sub-responsabile, il Responsabile dovrà svolgere una due diligence preliminare, per assicurare che esso abbia le capacità e le competenze necessarie per fornire il livello di protezione adeguato richiesto dalle normative in materia di trattamento dei dati personali e dal presente Accordo.

3.4 Qualora il Sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati personali, Il Responsabile conserva nei confronti del Titolare l'intera responsabilità per l'altrui inadempimento.

3.5. Il Responsabile non si avvarrà di Sub-responsabili situati al di fuori della Spazio Economico Europeo o che potrebbero trasferire i dati del Titolare al di fuori di esso, senza la previa autorizzazione scritta del Titolare. Il Responsabile, ove autorizzato, dovrà comunque garantire che

siano approntate garanzie adeguate in base agli artt. 46 e 47 GDPR, oppure che il trasferimento dei dati rientri in una delle deroghe previste dall'art. 49 del GDPR.

4. Misure di sicurezza tecniche e organizzative

4.1 Tenendo conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile dichiara di aver implementato le misure tecniche e organizzative utili per garantire un livello di sicurezza adeguato al rischio, ivi comprese le misure richieste dall'art. 32 del GDPR.

4.2 Il Responsabile si impegna altresì ad assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza dei Dati Personali di cui agli articoli da 32 a 36 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile.

5. Data breach

5.1 In caso di violazione dei dati personali, il Responsabile si impegna a comunicare al Titolare, senza giustificato ritardo e comunque entro 24 ore dal momento in cui ne viene a conoscenza, ogni violazione (avvenuta o probabile) che riguarda i dati personali, fornendo tutte le informazioni disponibili affinché il Titolare possa adempiere agli obblighi di notifica.

5.2 Con detta comunicazione il Responsabile deve, in particolare:

a. Descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b. Comunicare il nome e i dati di contatto del Responsabile della protezione dei dati personali o di altro punto di contatto dal quale possano essere acquisite informazioni;
c. Descrivere le probabili conseguenze della violazione;
d. Descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi;
e. Indicare le modifiche alla procedure e alle policy che intende adottare per evitare che l'evento od eventi simili possa nuovamente verificarsi, sottoponendo successivamente copia di tali modifiche al Titolare per la sua approvazione.

5.3 Il Responsabile dovrà comunque collaborare con il Titolare, assisterlo nel corso dell'indagine sulla violazione ed informarlo sulle azioni di mitigazione e sui rimedi adottati in risposta ad ogni problema relativo alla sicurezza dei dati personali.

6. Trasferimento di Dati Personali verso Paesi Terzi

Il Responsabile non tratterà né trasferirà i dati personali del Titolare al di fuori dell'Unione Europea (e dei paesi, settori e organizzazioni indicati come adeguati dalla Commissione Europea in quanto capaci di fornire una protezione adeguata dei dati) in assenza dell'autorizzazione scritta del Cliente.
Nel caso in cui il Responsabile effettui trattamenti di Dati Personali in un Paese Terzo che non sia stato oggetto di una decisione di adeguatezza ai sensi dell'art. 45 GDPR, le Parti convengono che si applicheranno le Clausole Contrattuali Tipo (titolare/responsabile) sottoscritte dalle Parti.
Nel caso in cui, nell'esecuzione del Contratto, il Responsabile debba trasferire dati personali a un Sub-responsabile localizzato in un Paese Terzo, il Responsabile – uniformemente a quanto già evidenziato all'art. 3 del presente Accordo – si assicurerà prima del trasferimento della presenza di meccanismi atti ad assicurare un livello di protezione adeguato, quali, alternativamente o congiuntamente: la sottoscrizione da parte del Responsabile e del Sub-responsabile delle Clausole Contrattuali Tipo, l'esistenza di norme vincolanti d'Impresa interne al Gruppo cui il Sub-responsabile appartiene, la sussistenza di una certificazione del Sub-responsabile in base al regime del Privacy Shield, l'esistenza di altre garanzie per il trasferimento di dati personali riconosciute dal GDPR.

7. Archivi non informatizzati (ove presenti)

Relativamente ai trattamenti eventualmente effettuati per mezzo di archivi non informatizzati, il Responsabile si impegna a:

a. garantire sicurezza e riservatezza ai locali che ospitano gli archivi contenenti dati di titolarità di AIFA;
b. assicurare che i relativi documenti siano custoditi in armadi dotati di chiave;
c. istituire un registro ove lasciare traccia di ogni accesso ai locali e ai documenti del personale autorizzato al trattamento, qualora ciò avvenga al di fuori dell'orario di lavoro;
d. munire gli uffici di apparecchi distruggi documenti per l'eliminazione fisica dei documenti cartacei.

8. Registro delle attività di trattamento

Il Responsabile – nei casi previsti dal GDPR – garantisce di avere adottato un registro che ricomprenda tutte le attività di trattamento effettuate per conto del Titolare, in conformità a quanto previsto dall'art. 30 del GDPR. Il Responsabile si impegna inoltre a mettere a disposizione del Titolare il registro, ove richiesto.

9. Cloud Computing

Nel caso in cui il Responsabile o i suoi Sub-responsabili si avvalgano di servizi di Cloud Computing, il Responsabile si impegna a: adeguarsi alle linee guida fornite dal Comitato Europeo per la Protezione dei Dati (o del Working Party Articolo 29), qualora applicabili al tipo di servizio svolto; garantire che i Dati Personali trattati per conto del Titolare siano isolati da quelli trattati per conto di altri clienti; assicurare che i dati personali oggetto del Contratto possano essere trasferiti, in formato standard e senza costi aggiuntivi per il Titolare, verso altre piattaforme e fornire al Titolare supporto per la realizzazione della migrazione; fornire al Titolare una lista di tutti i luoghi presso cui sono trattati (o potrebbero essere trattati) i dati personali, e, nel caso di trasferimento di dati personali verso paesi terzi, fornire evidenza della base giuridica che permette tale trasferimento e delle misure adottate a tutela dei dati personali. Il Responsabile avviserà il Titolare tempestivamente in caso di cambiamenti nei servizi di Cloud Computing di cui esso si avvale.

10. Durata della Nomina e obblighi successivi alla sua cessazione

10.1 Il presente Accordo sarà valido per il tempo necessario a svolgere le operazioni concernenti l'esecuzione dei Servizi e delle attività connesse al Contratto affidate al Responsabile e si considererà cessato a completamento di tale incarico e comunque alla cessazione, per qualsiasi causa, delle attività stesse.

10.2 Resta inteso che, al termine di tali attività, il presente Accordo non produrrà più alcun effetto ed il Responsabile dovrà cessare qualsiasi operazione di trattamento di dati personali per conto del Titolare.

10.3 Al termine delle attività di trattamento, il Responsabile, a scelta del Titolare, dovrà cancellare o restituire i dati trattati al Titolare e dovrà far sì che tali dati vengano cancellati o restituiti dal Sub-responsabile eventualmente nominato. In ogni caso, il Responsabile cancellerà (e farà cancellare dal Sub-responsabile eventualmente nominato) tutte le copie esistenti dei dati personali trattati per conto del Titolare, salvo che la loro conservazione sia prevista o imposta dalla legge.

10. 4 Il Responsabile dovrà attestare al Titolare, per iscritto, entro 15 giorni dalla cessazione del trattamento, di avere ottemperato a quanto previsto all'art. 10.3 del presente Accordo. Analoga attestazione, nello stesso termine, dovrà essere effettuata dal Responsabile per conto del Sub-responsabile.

11. Manleva ed indennizzo.
Il Responsabile s'impegna a tenere indenne e manlevare il Titolare da qualsiasi danno, pretesa di terzi o sanzione derivanti da azioni giudiziarie, arbitrali o amministrative di qualsiasi terzo, per le quali il Titolare possa essere ritenuto responsabile in conseguenza dell'inosservanza - da parte del Responsabile, del Sub-responsabile, di altro soggetto che operi sotto l'autorità del Responsabile o del Sub-responsabile - di quanto previsto dal GDPR, dalle altre normative in materia di protezione dei dati personali, dal presente Accordo o da qualsiasi altra istruzione impartita dal Titolare.

12. Disposizioni finali.
12.1 Quanto previsto dal presente Accordo non comporta alcun compenso in favore del Responsabile, aggiuntivo rispetto a quanto previsto nel Contratto.

12.2 La presente nomina è regolata dalla legge italiana. Ogni controversia che dovesse sorgere in relazione alla presente nomina, sarà devoluta alla esclusiva competenza del foro di Roma.

12.3 In caso di contrasto fra le disposizioni del Contratto e quelle della presente nomina, prevarranno le seconde.

12.4 In caso di invalidità o inefficacia di qualsiasi disposizione della presente nomina, le restanti disposizioni rimarranno valide ed efficaci.

12.5 Per quanto non espressamente previsto dalla presente nomina, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Il Titolare del trattamento
Agenzia Italiana del Farmaco
(f.to il Direttore Generale)

Per accettazione:

Il Fornitore - Responsabile Esterno del Trattamento

_____
(f.to il Legale Rappresentante)