ATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Ai sensi dell'art.28 del REG. (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati, GDPR)

TRA

L'IRCCS "FONDAZIONE G. PASCALE", con sede legale in Napoli (NA), via M. Semmola n.52, in persona del suo legale rappresentante, il Direttore Generale dott. A.M. Bianchi

TITOLARE DEL TRATTAMENTO DEI DATI (anche semplicemente Titolare)

E

RESPONSABILE DEL TRATTAMENTO DEI DATI (anche semplicemente Responsabile)

Con riferimento alle attività di trattamento dei dati inerenti:

- *inserire descrizione dei servizi come da contratto*

CONSIDERATO

- che l'art.4, par. 1, n. 8 GDPR definisce il "Responsabile del trattamento" come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento";

- che l'art.28 del Regolamento (UE) 2016/679 stabilisce che il trattamento effettuato per conto di un Titolare da parte del Responsabile è disciplinato da un contratto vincolante per il Responsabile nei confronti del Titolare, che definisce oggetto e durata del trattamento, natura e lo scopo, il tipo di dati personali e le categorie di interessati trattati, obblighi e diritti del Titolare;

- che l'art.28 GDPR, dispone che "*qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*"

- che il Responsabile, nell'ambito dei servizi affidati, ha i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza;

- che il Titolare intende affidare al Responsabile le attività di trattamento di dati personali come di seguito dettagliate e il Responsabile intende, altresì, eseguire il trattamento per conto del Titolare;

Sulla base di quanto sopra esposto, il Titolare e il Responsabile (di seguito anche Parti) convengono quanto segue.

ART. 1 – OGGETTO DELL'ACCORDO

Il Titolare e il Responsabile intendono disciplinare il trattamento dei dati personali da parte del Responsabile per conto del Titolare, specificando l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati e gli obblighi e i diritti reciproci.

Il Titolare, pertanto, impegna il Responsabile, che con la sottoscrizione accetta, a svolgere le operazioni di trattamento dei dati nell'esecuzione dei servizi sopra indicati, nei limiti delle funzioni e competenze attribuite.

ART. 2 – AMBITO DEL TRATTAMENTO

I dettagli del trattamento sui dati personali svolto dal Responsabile sono riportati nell'allegato A del presente atto di nomina.

ART. 3 – OBBLIGHI DEL RESPONSABILE

Il Responsabile del trattamento garantisce di possedere sufficienti conoscenze specialistiche, nonché affidabilità e risorse per attuare misure tecniche e organizzative che soddisfino i requisiti del GDPR.

Il Responsabile garantisce di trattare i dati personali per conto del Titolare, limitatamente alle attività di trattamento strettamente necessarie per l'espletamento delle funzioni attribuite, in esecuzione ai servizi sopra indicati.

Il Responsabile garantisce l'affidabilità di tutti gli operatori (dipendenti e/o collaboratori) che accedono ai dati personali trattati per conto del Titolare in base al presente Accordo e ed assicura, inoltre, che gli stessi abbiano ricevuto adeguate istruzioni ex art.29 del GDPR e che siano stati formati con riferimento alla protezione e gestione dei dati personali.

Il Responsabile assicura di attenersi, per sé, per i dipendenti e collaboratori di cui si avvale e per gli eventuali ulteriori Responsabili che intende individuare, alle regole comportamentali in tema di protezione dei dati personali eventualmente indicate dal Titolare o, in ogni caso, di tenere comportamenti conformi alle prescrizioni del GDPR.

Il Responsabile - tenuto conto del rischio per i diritti e le libertà degli interessati - si impegna ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio che comprendano, tra l'altro, le misure e le valutazioni di cui all'art.32 del GDPR come riportate in dettaglio nell'allegato B del presente atto di nomina.

Il Responsabile si impegna a rendere disponibili al Titolare tutte le informazioni necessarie a dimostrare la conformità agli obblighi stabiliti nel presente Accordo ed a consentire – su richiesta del Titolare - eventuali verifiche, comprese le ispezioni, svolte dal Titolare o da un organismo di controllo da questi nominato.

Il Responsabile del trattamento si impegna a fornire, secondo le modalità indicate dal Titolare, i dati e le informazioni necessari per consentire allo stesso di riscontrare eventuali ordini emessi dall'Autorità di Controllo o dalle Autorità Giudiziarie e/o di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante Privacy o all'Autorità Giudiziaria.

Il Responsabile del trattamento si impegna a redigere il registro dei trattamenti svolti, come da art. 30 GDPR, nonché a svolgere, in presenza delle condizioni previste dall'art. 35 del GDPR e di quelle ulteriori individuate dall'Autorità di controllo, la valutazione d'impatto, richiedendo anche il supporto del Titolare e a collaborare, nel modo più ampio, con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal GDPR.

ART. 4 – AMMINISTRATORI DI SISTEMA *(solo in caso di servizi di natura informatica)*

Per lo svolgimento dei servizi su indicati, il Responsabile si impegna a conformarsi al Provvedimento Generale del Garante per la protezione dei dati personali del 27.11.2008, così come modificato dal Provvedimento del Garante del 25.06. 2009 e *ss.mm.ii.* apportate dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.

Il Responsabile si impegna, in particolare, a:

a) procedere alla designazione individuale degli Amministratori di Sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti designati;

b) dare comunicazione al Titolare della/e nomina/e ad Amministratore di Sistema, specificando la/le persona/e nominata/e in tale veste, riportando per ciascun Amministratore di Sistema designato, o figura equivalente, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

c) nel caso di servizi di Amministrazione di Sistema affidati in *outsourcing* ad un sub-responsabile, il Responsabile deve conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratore di Sistema, nonché fornire al Titolare tutte le indicazioni di cui ai punti che precedono;

d) adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema o figure equivalenti. Le registrazioni dovranno essere conservate per un congruo periodo, comunque non inferiore a sei mesi.

ART. 5 – NOMINA DI ULTERIORI RESPONSABILI

Ai sensi dell'art. 28 commi 2 e 4 del GDPR, il Responsabile, qualora si avvalga di altri soggetti per lo svolgimento di attività (e conseguenti operazioni sui dati personali) per conto del Titolare, ha facoltà di ricorrere ad altri Responsabili, previa autorizzazione scritta generale del Titolare del trattamento.

Con il presente atto il Titolare conferisce al Responsabile il potere di nominare ulteriori Responsabili per dar corso alle attività oggetto dei servizi affidati, secondo il dettaglio riportato nell'Allegato C del presente atto. Il Responsabile del trattamento si impegna, comunque, a informare il Titolare circa l'eventuale nomina, l'aggiunta o la sostituzione di altri Responsabili del trattamento e a regolamentare i rapporti con gli altri Responsabili come previsto dall'art. 28 comma 4 e deve, pertanto, assicurare che il/i Responsabile/i di cui intende avvalersi è/sono in possesso dell'esperienza, della capacità e dell'affidabilità necessarie, presentano garanzie sufficienti, anche per la sicurezza del trattamento, di cui agli artt. 28 co.4 e 32 del GDPR.

Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile nominato con il presente Accordo conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

ART. 6 – DIRITTI E RICHIESTE DEGLI INTERESSATI

Il Responsabile del trattamento si impegna a comunicare ogni informazione utile al fine di aiutare il Titolare a rispettare i diritti degli Interessati, ai sensi degli artt.15-22 GDPR.

Nella misura in cui ciò sia possibile, il Responsabile del trattamento assiste il Titolare con adeguate misure tecniche e organizzative per l'adempimento dell'obbligo del Titolare di rispondere alle richieste di esercizio dei diritti degli Interessati.

In caso di esercizio dei predetti diritti, il Responsabile dà tempestiva comunicazione scritta, e comunque non oltre il termine di 5 giorni dalla richiesta, al Titolare, allegando una copia della richiesta dell'Interessato.

ART. 7 – TRASFERIMENTI VERSO PAESI TERZI

Il Responsabile del trattamento non può trasferire i dati personali provenienti dal Titolare al di fuori dello Spazio economico europeo (SEE), senza il previo consenso scritto e le istruzioni del Titolare, nel rispetto del presente Accordo e delle disposizioni atte a garantire la protezione dei dati personali di cui agli articoli del Capo V del GDPR, salvo che lo richieda il diritto europeo o nazionale cui è soggetto il Responsabile del trattamento. In tal caso il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

ART. 8 –VIOLAZIONE DEI DATI PERSONALI (cd. DATA BREACH)

In caso di violazione dei dati personali, il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo, ed in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza - della violazione. In tal modo, il Titolare dovrà provvedere a notificare la violazione al Garante privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare sarà tenuto, in base agli elementi di cui è venuto a conoscenza, anche grazie all'operato del Responsabile, a comunicare la violazione all'interessato.

In caso di violazione dei dati, il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto alle prescrizioni del GDPR e non ha adottato misure adeguate ai sensi dell'art. 32 del GDPR o ha agito in modo difforme o contrario rispetto a quanto riportato nel presente Accordo.

Il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

ART. 9 – CESSAZIONE DEL TRATTAMENTO

Questo Accordo diventerà effettivo dalla firma del Titolare e del Responsabile fino al termine dei servizi affidati al Responsabile o al termine del trattamento dei dati per qualsivoglia motivo.

Alla cessazione del trattamento dei dati, il Responsabile dovrà, a scelta del Titolare, restituire o cancellare i dati personali e le relative copie oggetto del trattamento dandone certificazione al Titolare, salvo che la legge preveda diversamente. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile del trattamento ne garantirà la riservatezza e si impegnerà a non procedere più al loro trattamento.

ART. 10 – LEGGE APPLICABILE E FORO COMPETENTE

Il presente Accordo, salvo quanto diversamente ivi previsto, in linea con il GDPR, è regolato dalle leggi della giurisdizione del Titolare.

La sede esclusiva per tutte le controversie derivanti da o in connessione con questo Accordo è il luogo di stabilimento del Titolare, fatto salvo il diritto di quest'ultimo di presentare un'azione giudiziaria contro il Responsabile, di fronte a qualsiasi altro tribunale ritenuto competente.

ART. 12 – RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (Data Protection Officer - DPO)

Il Titolare del trattamento si avvale di un Responsabile per la protezione dei dati personali (anche noto come Data Protection Officer -DPO), contattabile ai seguenti indirizzi: _____

Anche il Responsabile si avvale di un Responsabile per la protezione dei dati personali, contattabile ai seguenti indirizzi:

EMAIL: dpo@istitutotumori.na.it/ aggiungere eventuali altri _____

IL TITOLARE DEL TRATTAMENTO _____

Il RESPONSABILE _____

ALLEGATO A DELL'ATTO DI NOMINA A RESPONSABILE ESTERNO EX ART. 28 GDPR

DESCRIZIONE DEL TRATTAMENTO

a) Finalità: I dati relativi alle attività di trattamento sono trattati per le sole finalità relative all'incarico attribuito al Responsabile nell'esecuzione dei servizi oggetto dell'incarico:

- *dettagliare i servizi*
- *dettagliare le finalità*

b) Tipi di dati trattati: I dati personali trattati sono: *(specificare le tipologie di dati)*

- di tipo identificativo (es. nome e cognome, indirizzo di residenza, indirizzo email, codice fiscale, partita Iva, numero di telefono, etc.)

- di tipo particolare (atti a rivelare lo stato di salute, l'origine razziale ed etnica nonché, convinzioni religiose o filosofiche).

Il trattamento dei suddetti dati personali e, in special modo, quello dei dati particolari, deve avvenire nel rispetto dell'art.5 del GDPR.

d) Soggetti interessati: Le attività di trattamento e i relativi dati trattati interessano soggetti nella sfera della titolarità del Titolare, quali:

dettagliare le tipologie di interessati (ad es. dipendenti, collaboratori, fornitori, clienti, utenti, ecc.).

Il trattamento dei suindicati dati personali deve avvenire nel rispetto dei principi di liceità, correttezza e trasparenza.

e) Durata del trattamento: La durata delle attività di trattamento, e quindi il periodo di conservazione dei dati trattati, sarà limitato ad un arco di tempo non superiore al conseguimento delle finalità di cui alla lett. a) *(dettagliare eventuale tempistiche specifiche)* ed alla durata dell'incarico di servizio in essere, in ogni caso non oltre le tempistiche previste dalla Legge.

ALLEGATO B DELL'ATTO DI NOMINA RESPONSABILE ESTERNO EX. ART. 28 GDPR

MISURE TECNICHE ED ORGANIZZATIVE DEL RESPONSABILE

Il Responsabile e i suoi eventuali sub-responsabili per il trattamento dei dati, sulla base delle valutazioni dei rischi eseguite sul trattamento dei dati personali del Titolare, per garantire, in conformità all'art. 32 del GDPR, un livello di sicurezza adeguato devono mettere in atto e mantenere in essere appropriate misure tecniche e organizzative, controlli interni e processi di sicurezza intesi a proteggere i dati da perdita accidentale, distruzione o alterazione, da accessi o da diffusione non autorizzati o da illegale distruzione, e pertanto, in relazione alle specifiche attività di trattamento svolte per conto del Titolare, in particolar modo se dette attività vengono erogate presso le proprie strutture e sui propri sistemi. Tra i compiti del Responsabile, ai sensi dell'art. 28 del Regolamento UE 679/2016 par. 3 lett. h), vi è quello di mettere a disposizione del Titolare tutte le informazioni per dimostrare il rispetto degli obblighi e delle disposizioni previste dal su citato Regolamento.
Pertanto, per quanto attiene le misure tecniche ed organizzative il Responsabile deve disporre:

Riservatezza e formazione del personale

Tutto il personale con accesso ai dati deve essere adeguatamente formato su ruoli e responsabilità applicabili nella misura necessaria per svolgere le proprie funzioni lavorative, nonché sulle procedure legate alla riservatezza e alla sicurezza dei dati personali del Titolare in relazione alle diverse mansioni esercitate. I suddetti ruoli, con le annesse responsabilità, devono essere espressamente formalizzati con apposita nomina per iscritto.

Registro dei trattamenti

Ai sensi dell'art. 30 paragrafo 2 del GDPR il Responsabile deve tenere il registro di tutte le categorie di attività relative ai trattamenti svolti per conto del Titolare del trattamento.

Sicurezza fisica ed ambientale

Tutte le strutture in cui vengono trattati dati personali del Titolare devono essere protette con le migliori misure fisiche e ambientali per la protezione dei dati personali; l'accesso a tali aree deve essere concesso solo a persone autorizzate per scopi autorizzati.

Controllo logico accessi

L'accesso alle risorse informatiche che contengono dati personali del Titolare deve essere controllato da una adeguata politica degli accessi. Tale politica deve consentire l'accesso ai sistemi e ai dati limitatamente agli individui autorizzati alla gestione e solo per scopi di lavoro validi; deve definire le necessarie autorizzazioni sulla base dei ruoli e delle competenze attribuite. L'autenticazione per accedere alle risorse informative contenenti dati personali deve richiedere un identificativo unico.

Gestione dei sistemi

Devono essere implementati controlli anti-malware per contribuire a evitare che software dannosi possano accedere in modo non autorizzato ai dati personali del Titolare. Devono essere, altresì, implementati controlli per ridurre il rischio di accessi non autorizzati ai sistemi IT, quali firewall, e ciò anche per prevenire l'intercettazione non autorizzata o l'infiltrazione di dati personali in transito.

Sicurezza dei dati

Deve essere garantita la integrità e la disponibilità dei dati, nonché la continuità operativa dei sistemi e dei servizi di elaborazione attraverso procedure di backup e ripristino adeguate in linea con la criticità del sistema. Deve essere garantita la continuità operativa con un livello di operatività minimo e il ripristino nei termini previsti dal GDPR della piena funzionalità in caso di grave interruzione delle operazioni.

Valutazione d'impatto sulla protezione dei dati

Qualora le attività di trattamento svolte per conto del Titolare presentino un rischio elevato per i diritti e le libertà delle persone fisiche deve essere effettuata, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali secondo quanto prescritto dall'art.35 del GDPR.

Richieste degli interessati

Il Responsabile del trattamento, ai sensi degli artt. 15-22 GDPR, deve comunicare ogni informazione utile al fine di supportare il Titolare a rispettare i diritti degli Interessati con adeguate misure tecniche e organizzative per l'adempimento dell'obbligo del Titolare di rispondere alle richieste di esercizio dei diritti degli Interessati. In caso di esercizio dei predetti diritti, il Responsabile deve dare tempestiva comunicazione scritta al Titolare, e comunque non oltre il termine di 5 giorni dalla richiesta.

Incidenti di Sicurezza e Notifiche di Data Breach

Deve essere messa in atto una adeguata politica per la gestione degli incidenti legati alla privacy e alla sicurezza definendo ruoli e responsabilità dei soggetti incaricati alla gestione degli eventi, affinché possa esserne data tempestiva comunicazione al Titolare, in modo che possa provvedere a notificare la violazione al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Compliance

Le misure di sicurezza evidenziate devono essere monitorate regolarmente per garantire la continua conformità al GDPR.
Sempre nell'ottica di conformità al GDPR, i sistemi informatici per la erogazione dei servizi da parte del Responsabile devono essere certificati e validati dai preposti organismi e agenzie nazionali ed europei.

(sezione da inserire solo in caso di servizi di natura informatica)

Segue il dettaglio delle misure tecniche e organizzative, adottate dal Responsabile per garantire la sicurezza dei dati:

Elenco delle misure adottate (riempire solo in caso di misure adottate in concreto):

ID	*Tipologia di misure di sicurezza*	*Misura adottata*
1	*Misure di pseudonimizzazione e cifratura dei dati personali*	
2	*Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*	
3	*Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*	
4	*Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*	
5	*Misure di identificazione e autorizzazione dell'utente*	
6	*Misure di protezione dei dati durante la trasmissione*	

7	*Misure di protezione dei dati durante la conservazione*	
8	*Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati*	
9	*Misure per garantire la registrazione degli eventi*	
10	*Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita*	
11	*Misure di informatica interna e di gestione e governance della sicurezza informatica*	
12	*Misure di certificazione/garanzia di processi e prodotti*	
13	*Misure per garantire la minimizzazione dei dati*	
14	*Misure per garantire la qualità dei dati*	
15	*Misure per consentire la portabilità dei dati e garantire la cancellazione*	

ALLEGATO C DELL'ATTO DI NOMINA RESPONSABILE ESTERNO EX. ART. 28 GDPR

ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

Il presente allegato deve essere compilato in caso di utilizzo di sub-responsabili del trattamento

Dati dei subresponsabili autorizzati allo svolgimento delle attività di trattamento dati di cui ai servizi affidati al Responsabile:

Denominazione del subresponsabile	*Indirizzo*	*Descrizione dell'attività*