ACCORDO DI CONTITOLARITÀ PER IL TRATTAMENTO DEI DATI PERSONALI TRA OSR E TELETHON

Ospedale San Raffaele S.r.l., con sede in Milano – Via Olgettina n. 60, (di seguito, "**OSR**") e **Fondazione Telethon,** con sede in Roma, via Varese 16 B - (di seguito "**Telethon**") in data 18 gennaio 2021 hanno sottoscritto un accordo di contitolarità **ai sensi dell'art. 26 Regolamento EU 679/2016** (di seguito **"Accordo"**) **per** regolamentare il rapporto tra loro in riferimento al trattamento dei dati personali e particolari dei soggetti interessati quali pazienti, fornitori, nonché di dipendenti, docenti, ricercatori, consulenti e collaboratori effettuato, in relazione alle attività di ricerca indicate nelle premesse alla lett. e) ed f) dalle risorse umane contrattualizzate da Telethon e OSR ovvero da collaboratori di soggetti terzi, quali FCSR e UniSR, i quali prestano la propria opera presso le strutture del Tiget ed hanno stipulato una convenzione per tali attività con OSR.

Si riportano qui a seguire i contenuti essenziali dell'Accordo al fine dei darne informazione ai soggetti interessati ad integrazione della informativa privacy loro rilasciata.

1. **Categorie di dati trattati e basi giuridiche**

1.1 La contitolarità qui regolamentata è riferita all'insieme delle operazioni di trattamento dei **dati personali e particolari dei pazienti** (dati anagrafici, dati di contatto, dati relativi alla salute, dati genetici) per finalità clinica e di ricerca condotta dai soggetti contrattualizzati dalle Parti e da soggetti terzi che operano presso le strutture del Tiget, ed in particolare per i progetti di ricerca di cui alle lett. e) ed f) indicati nelle premesse; alle operazioni di trattamento dei **dati personali e particolari dei soggetti contrattualizzati da OSR e Fondazione**, quali docenti, ricercatori, consulenti, collaboratori, **e di collaboratori di soggetti terzi** (dati anagrafici, dati di contatto, titoli di studio, dati relativi a condanne penali e reati, dati relativi alla salute, dati che rilevano l'appartenenza sindacale) che prestano la propria opera presso le strutture del Tiget per le attività sopracitate ed infine alle operazioni di trattamento dei **dati personali di fornitori di beni e servizi**, tutte espresse nell'apposita informativa che le Parti rilasceranno ai soggetti interessati secondo il testo tra loro condiviso.

1.2 La base giuridica sottostante l'acquisizione dei dati personali e particolari dei soggetti interessati, quali i pazienti, è costituita dal rilascio del consenso (art.6 par. 1 lettera a)

GDPR e art. 9 par. 2, lettera a), finalizzato al trattamento da parte di OSR e Telethon dei dati personali e particolari degli interessati per fini di ricerca scientifica, le cui attività sono condotte dalle risorse presso le strutture del Tiget. Il consenso dell'interessato non sarà necessario nei casi in cui ricorrano i presupposti di cui all'art. 9, comma 2, lett. j), oppure quelli indicati nell'Autorizzazione Generale dell'Autorità Garante 9/2016 e nel provvedimento della medesima Autorità 146/2019, nel rispetto delle indicazioni di cui agli artt. 110 e 110 bis del D.Lgs. 196/2003.

1.3 La base giuridica sottostante l'acquisizione dei dati personali e particolari dei soggetti interessati, vale a dire i soggetti contrattualizzati da OSR e Fondazione (docenti, ricercatori, consulenti, collaboratori) e i collaboratori di soggetti terzi FCSR e UniSR, i quali prestano la propria opera presso le strutture del Tiget, è costituita dall'esecuzione di un contratto di cui l'interessato è parte (art.6 par. 1 lettera b) GDPR), consistente nell'instaurazione di un rapporto di lavoro per le attività di ricerca sopracitate e dalla gestione degli obblighi in materia di salute e sicurezza sul posto di lavoro (art. 9 par.2 lettera b) GDPR)

1.4 È costituita invece dall'adempimento degli obblighi legali ai quali sono soggetti i contitolari (art. 6 par. 1 lett. c) GDPR) la base giuridica del trattamento, eseguito da OSR e Telethon, dei dati comuni dei soggetti interessati, ossia le risorse di OSR e Telethon (quali docenti, ricercatori, consulenti, collaboratori) e collaboratori di soggetti terzi FCSR e UniSR. Per quanto concerne i dati di natura particolare il presupposto di liceità è rappresentato dalla necessità di assolvere gli obblighi ed esercitare i diritti specifici del titolare dei contitolari del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9 par.2 lett. b) GDPR).

1.5 Infine, la base giuridica sottostante l'acquisizione dei dati personali dei soggetti interessati, quali i fornitori di servizi, è costituita dall'esecuzione di un contratto di cui l'interessato è parte (art.6 par. 1 lettera b) GDPR), consistente nell'instaurazione di un rapporto di fornitura di servizi strettamente correlato alle attività di ricerca sopraccitate, nonché dall'adempimento degli obblighi legali ai quali sono soggetti i contitolari (art. 6 par. 1 lett. c) GDPR).

2. Le informazioni sul trattamento dei dati

2.1 I Contitolari provvedono a rispettare gli obblighi di informazione nei confronti degli interessati fornendo agli stessi tutte le informazioni prescritte ai sensi dell'art. 13 del Regolamento e le comunicazioni di cui ex artt. 15 a 22 e art. 34 GDPR, relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un

linguaggio semplice e chiaro; le informative verranno realizzate congiuntamente dalle parti e fornite per iscritto o con l'ausilio di mezzi elettronici e corredate da un estratto del presente accordo.

2.2 L'informativa di cui all'art. 13 del GDPR sarà fornita dall'OSR ai pazienti, ai propri dipendenti (compresi i collaboratori di FCSR e UniSR) ai fornitori, quali soggetti interessati, mentre sarà fornita da Telethon ai propri dipendenti (docenti, ricercatori, consulenti, collaboratori), quali soggetti interessati. Il consenso al trattamento e alla comunicazione dei dati personali del soggetto interessato sarà acquisito rispettivamente da OSR e ciascuna parte provvederà alla relativa registrazione secondo le proprie modalità interne.

2.3 In merito, le Parti concordano nel fornire, all'atto della raccolta dei dati personali presso l'interessato, tutte le informazioni di seguito elencate:

- **a.** l'identità e i dati di contatto dei contitolari del trattamento;
- **b.** i dati di contatto del responsabile della protezione dei dati;
- **c.** le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- **d.** i destinatari e le categorie di destinatari dei dati personali;
- **e.** il periodo di conservazione dei dati personali;
- **f.** l'eventuale intenzione della parte di trasferire dati personali all'estero (extra UE);
- **g.** l'esistenza del diritto dell'interessato di chiedere ai contitolari del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- **h.** qualora il trattamento sia basato sull'articolo 6 GDPR, paragrafo 1, lettera a), oppure sull'articolo 9 GDPR, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- **i.** il diritto di proporre reclamo a un'autorità di controllo;
- **j.** se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

k. l'esistenza di un accordo di contitolarità il cui contenuto essenziale viene messo a disposizione degli interessati presso la sede dell'OSR, individuato quale punto di contatto per gli interessati nell'ambito dell'accordo di contitolarità;

l. la condivisione del trattamento dei dati tra contitolari nel rispetto dell'accordo di cui al punto k).

Ciascuna Parte fornirà ai soggetti incaricati al trattamento una specifica autorizzazione al trattamento di dati personali.

3. Garanzie per i diritti degli interessati

3.1 Le Parti convengono che i reclami e le richieste di esercizio dei diritti presentati dai soggetti interessati per i trattamenti di dati che rientrano nell'ambito di contitolarità definito dal presente Accordo, saranno raccolti, gestiti e curati dall'OSR. A tal fine, il suddetto si impegna a mettere a disposizione degli stessi la casella di posta elettronica dpo@hsr.it cui gli interessati possono far pervenire le loro richieste e/o pretese, fermo restando, in ogni caso, che gli stessi potranno esercitare i propri diritti sia nei confronti dell'OSR sia di Telethon, ai sensi dell'art. 26, comma 3, del Regolamento, convenendo ciascuna Parte, indipendentemente dall'altra, dinanzi al Garante della protezione dei dati personali e/o la giustizia nazionale.

3.2 Le Parti si danno reciprocamente atto che coopereranno al fine di garantire il diritto dell'interessato. In tal senso, ciascuna Parte si impegna a trasmettere tempestivamente comunque non oltre 7 giorni lavorativi le richieste di esercizio dei diritti all'altra Parte, fornendo tutte le informazioni necessarie, ove non in possesso di quest'ultimo. La Parte che ha ricevuto la richiesta da parte dell'interessato si impegna a rispondere alla stessa senza ritardo, e comunque entro e non oltre 30 giorni ai sensi dell'art. 12 par. 3 GDPR, di concerto con l'altra parte.

3.3 Ciascuna Parte sarà tenuta a comunicare all'altra ogni rettifica o cancellazione di dati personali o limitazione del trattamento in conformità con il Regolamento e qualsivoglia normativa applicabile, nei limiti richiesti da tale normativa e, altresì, ogni eventuale revoca di consenso presentata dagli interessati in relazione alle finalità di trattamento che richiedono quale base giuridica il consenso dell'interessato (ivi inclusi i trattamenti di dati rientranti nelle particolari categorie di cui all'art. 9 del GDPR).

4. Riservatezza, misure di sicurezza e privacy by design-by default

4.1 Le Parti, ciascuno per quanto di propria competenza, si danno reciprocamente atto di avere adottato e di revisionare regolarmente le misure tecniche e organizzative

adeguate alle prescrizioni del Regolamento, tenuto conto della natura del trattamento da ciascuno di essi effettuato e delle informazioni a disposizione di ciascuna Parte, al fine di garantire un livello di sicurezza adeguato ai rischi di cui al GDPR ed alla normativa italiana in materia di trattamento di dati personali.

4.2 Eventuali variazioni delle misure di sicurezza che si rendessero necessarie a causa di modifiche e aggiornamenti della normativa in materia di protezione dei dati personali, mutamenti inerenti alla tipologia, alla natura, al contesto, alla finalità del trattamento, nonché a causa di variazioni del rischio o dell'evoluzione tecnologica delle applicazioni utilizzate, saranno adottate e implementate autonomamente da ciascuna Parte.

4.3 In particolare, l'OSR garantisce che le misure tecniche ed organizzative implementate assicurano la continua riservatezza, integrità, disponibilità e resilienza dei propri sistemi e dei servizi che trattano i dati personali e sono adeguate anche al fine di permettere il ripristino tempestivo della disponibilità e dell'accesso ai dati in caso di incidente fisico o tecnico.
4.4 L'OSR si impegna, inoltre, a fornire sufficiente documentazione all'altra parte (se richiesto) nonché ad eseguire un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio.

7.5 Le Parti, altresì, garantiscono, nell'ambito della loro sfera di influenza, che tutto il personale coinvolto nel trattamento dei dati:

- manterrà la riservatezza dei dati ai sensi degli Artt. 28.3, 29 e 32 del GDPR, per tutta la durata del loro rapporto lavorativo, nonché per il tempo successivo alla sua cessazione;
- è adeguatamente formato sulle disposizioni in materia di protezione dei dati (GDPR e normativa nazionale, nel caso italiano il Codice Privacy – D. Lgs. 196/2003);

4.6 Gli stessi Contitolari assicurano il rispetto dei principi della protezione dei dati fin dalla progettazione (Privacy-by-Design ex art. 25 par.1 GDPR) e dei principi della protezione dei dati per impostazione predefinita (Privacy-by-Default ex art. 25 par. 2 GDPR), utilizzando misure tecniche e organizzative adeguate al caso concreto.

5. Data Breach

5.1 Ciascuna Parte darà tempestivamente notizia all'altra, entro 24 ore e comunque non oltre i termini di legge, di un'eventuale violazione o pericolo per la riservatezza,

completezza ed integrità dei dati personali trattati, occorsi nel rispettivo ambito di competenza e applicazione.

5.2 La procedura di notifica di Data Breach al Garante Privacy verrà gestita dall'OSR, senza alcun ritardo e, comunque, entro 72 ore dal momento in cui ne è venuto a conoscenza e nell'osservanza e rispetto degli obblighi di comunicazione di cui all'art. 33 del Regolamento.

5.3 Le Parti si danno reciprocamente atto che coopereranno al fine di:

- rimediare adeguatamente alle conseguenze della violazione, limitando e minimizzando gli effetti dannosi;
- adottare tutte le misure necessarie per evitare il ripetersi di tali eventi pregiudizievoli.

6. Registro dei Trattamenti

I Contitolari convengono che, le attività di trattamento di cui al medesimo Accordo dovranno essere inserite nei rispettivi Registri dei trattamenti, adottati e manutenuti regolarmente da ciascuna Parte, ai sensi dell'art. 30 del GDPR.

7. Responsabili del trattamento, Autorizzati al trattamento e Amministratori di sistema

7.1 Le Parti designano, mediante apposito atto scritto, i Responsabili del Trattamento in ordine a quei trattamenti che rientrano nell'ambito di contitolarità del predetto Accordo.

7.2 I Contitolari, ciascuno per quanto di propria competenza, provvedono ad individuare e a designare mediante atto iscritto i soggetti Autorizzati al trattamento, vale a dire tutte le persone fisiche autorizzate ad accedere e a trattare i dati personali e particolari rientranti nell'ambito di contitolarità del predetto Accordo, e gli Amministratori di sistema. In particolare:

- L'OSR designerà quali Autorizzati al trattamento le proprie risorse contrattualizzate che svolgono attività di ricerca presso le strutture del Tiget, e come Amministratori di sistema tutte quelle figure professionali contrattualizzate deputate alla gestione e alla manutenzione degli impianti di elaborazione/sistemi informativi o dei relativi componenti;
- Telethon designerà quali Autorizzati al trattamento le proprie risorse contrattualizzate (docenti, ricercatori, consulenti, collaboratori) che svolgono attività di ricerca presso le strutture del Tiget.

Qualora dalla individuazione dei soggetti autorizzati dovesse discendere l'attivazione di specifiche utenze di sistemi informatici, ciascuna contitolare detentore dei sistemi attiverà tali utenze sulla base delle indicazioni ricevute dalla parte che avrà provveduto alla designazione dei medesimi soggetti autorizzati

7.3 I Contitolari devono altresì individuare diversi livelli di trattamento in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore.

7.4 Contestualmente alla designazione, i Contitolari si fanno carico di fornire istruzioni scritte e dettagliate, nonché specifiche procedure alle figure sopra indicate circa le modalità del trattamento, in ottemperanza a quanto disposto dalla legge.

8. Messa a disposizione del contenuto essenziale dell'accordo agli interessati

Le Parti si impegnano altresì, ai sensi dell'art. 26, comma 2, del GDPR, a mettere a disposizione dell'interessato il contenuto essenziale del presente Accordo di contitolarità, come allegato dell'informativa resa agli interessati e consultabile agli indirizzi web di cui al superiore art. 5.

9. Durata

La durata del presente Accordo è legata alla durata del Contratto e si intenderà automaticamente risolta alla scadenza del Contratto, salva la sopravvivenza degli obblighi necessari di natura legale e regolamentare in materia di trattamento di dati personali.

10. Responsabilità

10.1 Al fine di definire le loro responsabilità, le Parti si obbligano in via solidale per eventuali danni arrecati agli interessati a causa del trattamento eseguito in contitolarità, pertanto, ciascuna di esse dovrà risarcire *in toto* l'interessato che dimostra di essere stato danneggiato.

10.2 Ferma restando la possibilità di ciascun interessato ad esercitare i propri diritti nei confronti di ciascun contitolare del trattamento, la Parte che ha risarcito in tutto o in parte l'interessato ha facoltà di esercitare un diritto di rivalsa nei confronti dell'altra, responsabile effettiva del danno che ha assunto una responsabilità così come delineata nel presente accordo, esercitando l'azione di regresso.

11. Trattamenti come autonomi titolari

11.1 Le Parti si danno altresì reciprocamente atto che, in pendenza del presente Accordo potranno trovarsi ad effettuare trattamenti in maniera autonoma ed in nessun

caso connessi alle attività di cui all'accordo di contitolarità qui disciplinato, nel qual caso Telethon e OSR riconoscono sin d'ora la loro qualità di Titolari autonomi del trattamento, e pertanto ciascuna Parte sarà autonomamente responsabile dei relativi adempimenti e delle violazioni relative alla normativa vigente.

11.2 Qualora OSR fosse coinvolto quale centro partecipante e/o coordinatore all'interno di studi/sperimentazioni promossi da soggetti terzi (rispetto al presente accordo) ed in tale contesto dovesse avvalersi della collaborazione di Telethon, i dati personali eventualmente necessari allo svolgimento dell'attività verrebbero trattati da quest'ultima in qualità di Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento 679/2016/UE.