

DECRETO DEL DIRETTORE GENERALE N. 1156 del 06/05/2025 - Allegato Utente 2 (A02)
**ATTO DI NOMINA
DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI**
(ai sensi dell'art. 28 del Regolamento UE 2016/679)

L'IRCCS Ospedale Policlinico San Martino, con sede legale in Genova, Largo Rosanna Benzi 10 - 16132, C.F./P. IVA n. 02060250996, in qualità di Titolare del trattamento dei dati personali (di seguito **Policlinico** o **Titolare**) nella persona del suo Rappresentante Legale, il Direttore Generale Dott. Marco Damonte Prioli,

PREMESSO CHE

- Con deliberazione n. 528 del 26.03.2025 è stato approvato *il rinnovo della convenzione* con la Fondazione IRCCS Cà Granda Ospedale Maggiore Policlinico con sede legale a Milano in via Francesco Sforza n. 28 P.IVA/C.F. 04724150968 avente ad oggetto attività di prelievo e trapianti d'organo con scadenza il 31.12.2026;
- per l'esecuzione del rapporto giuridico sopra individuato e per il compimento delle attività conseguenti, la ditta/società esegue necessariamente operazioni di trattamento di dati personali per conto del Policlinico;
- l'art. 28 del Regolamento (UE)2016/679 sulla protezione dei dati personali, di seguito GDPR, dispone che qualora un trattamento sia effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che garantiscano l'adozione di misure tecniche ed organizzative adeguate, in modo tale che il trattamento sia conforme alla normativa in materia di protezione dati e garantisca la tutela dei diritti dell'interessato;
- la delega di tali attività di trattamento, in conformità al disposto dall'art. 28 del GDPR, deve essere disciplinata da un contratto o da altro atto giuridico che vincoli il Responsabile al Titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- il Responsabile, sottoscrivendo l'atto giuridico sopracitato, garantisce al Titolare di essere in possesso di conoscenze specialistiche, di possedere i requisiti di esperienza, capacità e affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di protezione dei dati, ivi compreso il profilo relativo alla sicurezza e la tutela dei diritti degli interessati;

Tutto ciò premesso, costituendo parte integrante e sostanziale del presente atto,

NOMINA

**la Fondazione IRCCS Cà Granda Ospedale Maggiore Policlinico
RESPONSABILE DEL TRATTAMENTO**

relativamente alle attività di trattamento necessarie all'esecuzione del rapporto giuridico riportato in premessa e descritto (sezione I) nel prosieguo del presente atto.

La Fondazione, Responsabile del trattamento dei dati personali, ha il compito e la responsabilità

di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia di trattamento dei dati personali ed è tenuta a rispettare le seguenti istruzioni operative (sezione II), osservando scrupolosamente le indicazioni impartite con il presente atto nonché con le successive modifiche o integrazioni.

La nomina di Responsabile del trattamento dei dati personali decade automaticamente alla scadenza o alla risoluzione del rapporto instaurato con il Titolare. Nel caso di durata del trattamento eccedente la durata del rapporto sottostante, la qualifica di Responsabile è mantenuta per tutta la durata del trattamento, come disciplinato dall'art. 2, e non oltre.

Sezione I

DESCRIZIONE DEL TRATTAMENTO

ART. 1 – ATTIVITÀ DEL TRATTAMENTO

Con il presente atto al Responsabile è attribuito il compito di effettuare le operazioni di trattamento dei dati personali al fine di svolgere le seguenti attività:

- funzioni di coordinamento dei trapianti di tipo Standard e di tipo Speciale (liste d'attesa, coordinamento del processo di trapianto e gestione del rischio clinico, coordinamento programmi di carattere nazionale, dati di attività, aggiornamento permanente);
- prestazioni di laboratorio di tipo Standard e di tipo Speciale (nuovi pazienti e pazienti in lista, idoneità donatori e compatibilità ricevente).

Il trattamento di dati personali affidato al Responsabile, che può svolgersi con modalità elettronica e manuale, è finalizzato esclusivamente all'esecuzione delle attività sopra indicate, per le quali i dati saranno trattati solo se necessari, pertinenti e non eccedenti.

Al Responsabile è pertanto vietato ogni ulteriore trattamento di tali dati personali, in particolare se effettuato per finalità diverse da quelle per cui i dati sono stati conferiti, quali per esempio marketing, studio e ricerca.

Il Responsabile risponderà quindi di tutti i danni eventualmente cagionati ai diritti, alle libertà e alla dignità degli Interessati qualora esegua un trattamento per finalità ulteriori non collegate al servizio fornito o non rispetti le indicazioni fornite.

ART. 2 - DURATA DEL TRATTAMENTO

Le attività di trattamento dei dati personali sono consentite al Responsabile per tutta la durata del rapporto giuridico, così come specificato in premessa, fatto salvo il maggior tempo di conservazione dei dati per il solo periodo strettamente necessario al compimento di eventuali attività amministrative correlate agli adempimenti contrattuali (rendicontazione, verifica, controllo, ecc.).

Il Responsabile è autorizzato a conservare i dati oggetto di trattamento per il tempo strettamente necessario allo svolgimento delle prestazioni concordate; in particolare, questi non può trattenere copie cartacee o elettroniche dei dati e della documentazione oggetto di affidamento, che dovranno essere restituiti qualora ne ricorrano i presupposti previsti dalla legge o dall'atto giuridico stipulato o se comunque ciò sia reso necessario dalla revoca del consenso al trattamento dei dati da parte del singolo Interessato.

Il Responsabile si impegna anche a restituire prontamente al Titolare i dati qualora da questi richiesto. In ogni caso il Responsabile è tenuto alla cancellazione di tutti i dati contenuti nei propri archivi fisici e informatizzati, compresi quelli memorizzati dal sistema di backup, salvo diverse disposizioni di legge, al termine del rapporto.

Al termine del rapporto il Responsabile è tenuto, inoltre, a dichiarare formalmente al Titolare

tramite apposita comunicazione PEC, entro un mese dalla cessazione del rapporto, di avere provveduto alla succitata cancellazione.

ART. 3 - TIPO DI DATI PERSONALI OGGETTO DI TRATTAMENTO

I dati personali trattati dal Responsabile sono:

- ☐ X Dati anagrafici (nome, cognome, sesso, data e luogo di nascita, codice fiscale, residenza, domicilio, altro)
- ☐ X Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ X Dati relativi a documenti di identificazione/riconoscimento (carta di identità, patente, CNS, altro)
- ☐ Dati di accesso e di identificazione (username, password, *customer ID*, altro...)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro...)
- ☐ Dati di profilazione
- ☐ Dati di localizzazione
- ☐ Dati relativi a condanne penali e reati o a connesse misure di sicurezza o di prevenzione
- ☐ X Dati appartenenti alle categorie particolari di cui all'art. 9 del Reg. UE 2016/679 e, nello specifico:
 - ☐ X dati relativi alla salute
 - ☐ dati relativi alla vita sessuale/orientamento sessuale
 - ☐ X dati genetici
 - ☐ X dati biometrici
 - ☐ dati relativi a origine razziale/etnica
 - ☐ dati relativi ad opinioni politiche o convinzioni religiose/filosofiche
 - ☐ dati relativi all'appartenenze sindacale
- ☐ altro (specificare) _____

ART. 4 - CATEGORIE DI INTERESSATI

Il Responsabile è autorizzato a trattare dati personali appartenenti alle seguenti categorie di Interessati:

- ☐ Dipendenti
- ☐ Consulenti/Collaboratori
- ☐ Utenti/Contraenti
- ☐ Beneficiari o assistiti
- ☐ XPazienti
- ☐ Minori
- ☐ XLegali rappresentanti (genitori, amministratori di sostegno, tutori, ecc...)
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Altro (specificare)_____

Sezione II

Istruzioni del Titolare

ART. 5 - OBBLIGHI GENERALI

Il Responsabile del trattamento è tenuto a collaborare con il Titolare per garantire il rispetto della normativa in materia di protezione dei dati personali, ed in particolare a trattare i dati personali:

- nel rispetto dei generali principi di liceità, correttezza e trasparenza, soltanto se necessari e pertinenti all'esecuzione del trattamento affidato e in ogni caso per il periodo minimo necessario;
- nel rispetto del principio di minimizzazione evitando in particolare duplicazioni non necessarie;
- adottando misure adeguate di sicurezza tecniche ed organizzative, che assicurino la protezione dei dati personali e la tutela dei diritti, delle libertà e della dignità degli Interessati;
- mettendo a disposizione del Titolare ogni informazione necessaria a dimostrare il rispetto degli obblighi di cui al presente atto, comprese quelle necessarie a fornire, entro 24 ore dalla richiesta, riscontro alle richieste degli Interessati e alle istanze dell'Autorità Garante per la protezione dei dati personali, fornendo ogni informazione a tal fine richiesta;
- consentendo ogni attività di revisione, audit e controllo, comprese le ispezioni del Titolare o di un altro soggetto da questi incaricato previo congruo preavviso;
- comunicando al Titolare, entro 24 ore dall'avvenuta conoscenza, qualsiasi incidente di sicurezza o violazione di dati personali di cui al punto 12 dell'articolo 4 del GDPR, ossia ogni violazione di sicurezza che comporti l'accidentale o illecita distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati (*data breach*);
- comunicando tempestivamente al Titolare, senza ingiustificato ritardo e comunque entro il termine massimo di 24 ore da quando ne è venuto a conoscenza, ogni incidente che ha un impatto significativo sulla fornitura dei servizi erogati dal Responsabile, al fine di avviare il procedimento formale di comunicazione nei confronti del CSIRT (Computer Security Incident Response Team) Italia, ai sensi degli art. 25 e 26 del D.Lgs. 4 settembre 2024 n.

138 (Attuazione della Direttiva UE 2022/2555) e della Legge n.90 del 28 giugno 2024 recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”;

- comunicando tempestivamente ed in maniera proattiva al Titolare ogni notizia rilevante ai fini della tutela della riservatezza e protezione dei dati, informandolo immediatamente qualora ritenga che un’istruzione impartita per il trattamento violi le norme in materia di trattamento di dati personali;
- inoltrando al Titolare entro il 31 gennaio di ogni anno una relazione che evidenzi lo stato dell’arte del rispetto delle disposizioni impartite con il presente atto o con atti successivi;
- il Responsabile del trattamento non è autorizzato ad effettuare alcuna attività di trattamento per finalità diverse da quelle indicate nel presente atto; un eventuale trattamento con finalità diverse viola il disposto del paragrafo 3 dell'articolo 28 del GDPR e il mandato conferito dal Titolare del trattamento, e il Responsabile si configurerà come autonomo Titolare, (punto 81 delle Linee Guida 07/2020 sui concetti di Titolare del trattamento e di Responsabile del trattamento ai sensi del GDPR adottate il 7 luglio 2021);
- eventuali trattamenti difforni da quelli autorizzati a mezzo del presente atto costituiscono inadempimenti contrattuali di non scarsa rilevanza e violazioni del mandato conferito, con facoltà per il Titolare di esercitare il diritto di risoluzione del contratto per inadempimento, con ogni conseguente effetto a carico del Responsabile;
- qualora da un’attività di verifica del Titolare del trattamento dovesse emergere un trattamento di dati illecito per riuso di dati personali, questo procederà a segnalare l’episodio all’Autorità Garante.

ART. 6 - OBBLIGHI DI ADOZIONE DI MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE

Il Responsabile si impegna, inoltre, al fine di assicurare un livello di sicurezza adeguato al rischio, ad adottare adeguate misure tecniche e organizzative, anche in conformità all’articolo 32 del GDPR, volte a garantire che:

- il trattamento dei dati personali sia effettuato soltanto da parte dei propri collaboratori e nel caso intenda avvalersi, anche per attività di conservazione o trattamento attraverso software, hardware o sistemi informativi in cloud, di altri soggetti, siano rispettate le indicazioni succitate;
- i locali in cui siano eventualmente trattati o conservati i dati personali o i dispositivi utilizzati per la loro archiviazione in formato elettronico presentino tutte le garanzie di sicurezza strutturale e tecnica per prevenire il danneggiamento, la perdita o l’acquisizione illecita dei dati da parte di terzi;
- siano assicurate su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi utilizzati per il trattamento dei dati personali;
- sia predisposto e mantenuto aggiornato il registro delle attività di trattamento ai sensi del comma 2 dell’articolo 30 del GDPR, identificando e censendo i trattamenti di dati personali operati per conto del Titolare nonché le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all’espletamento delle attività oggetto di delega;
- siano adottate tutte le misure previste dal provvedimento dell’autorità di controllo del 27 novembre 2008 relativo a “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”.

ART. 7 - SUB-RESPONSABILI DEL TRATTAMENTO DI CUI AL PARAGRAFO 2 DELL'ARTICOLO 28 DEL GDPR

Il Responsabile del trattamento non può avvalersi di un sub-Responsabile del trattamento per lo svolgimento delle attività di trattamento da effettuare per conto del Titolare del trattamento senza la previa autorizzazione specifica scritta del Titolare del trattamento. Il Responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno 30 giorni prima di ricorrere ad un sub-Responsabile del trattamento, unitamente alle informazioni necessarie per consentire al Titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento deve essere mantenuto aggiornato.

Il Responsabile del trattamento che ricorre a un sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento, stipula un contratto che impone al sub-Responsabile del trattamento gli stessi obblighi in materia di protezione dei dati imposti al Responsabile del trattamento conformemente alle presenti clausole. Il Responsabile del trattamento si assicura che il sub-Responsabile del trattamento rispetti gli obblighi cui il Responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679.

Su richiesta del Titolare del trattamento, il Responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-Responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

Il Responsabile del trattamento rimane pienamente responsabile, nei confronti del Titolare del trattamento, dell'adempimento degli obblighi del sub-Responsabile derivanti dal contratto che questi ha stipulato con il Responsabile del trattamento. Il Responsabile del trattamento notifica al Titolare qualunque inadempimento, da parte del sub-Responsabile del trattamento, degli obblighi contrattuali.

ART. 8 - INOSSERVANZA DEL PRESENTE ATTO E RISOLUZIONE

Fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il Responsabile del trattamento violi gli obblighi che gli incombono dal presente atto, il Titolare del trattamento può dargli istruzione di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti il presente atto o non sia risolto il contratto. Il Responsabile del trattamento informa prontamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare il presente atto.

Il Titolare del trattamento ha diritto di risolvere il rapporto sottostante, per quanto riguarda il trattamento dei dati, qualora:

- 1) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare per violazione del presente atto e il rispetto del presente atto non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
- 2) il Responsabile del trattamento violi in modo sostanziale o persistente il presente atto o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;
- 3) il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità alle presenti clausole o al Regolamento (UE) 2016/679;

Il Responsabile del trattamento ha diritto di risolvere il rapporto sottostante, per quanto riguarda il trattamento dei dati personali, a norma del presente atto qualora, dopo aver informato il Titolare del trattamento che le sue istruzioni violano il Regolamento (UE) 2016/679, il Titolare del

trattamento insista sul rispetto delle istruzioni da parte del Responsabile.

ART. 9 - RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

Il Responsabile, all'atto della scadenza del rapporto sottostante o, comunque, in caso di cessazione - per qualunque causa - dell'efficacia del presente atto di nomina, salva la sussistenza di un obbligo di legge che ne preveda la conservazione, dovrà interrompere ogni operazione di trattamento e dovrà provvedere alla restituzione dei dati trattati ed alla cancellazione di eventuali copie detenute.

Eventuali copie, salvo diversi accordi che potranno intervenire alla cessazione del rapporto, dovranno essere distrutte entro tempi compatibili con le ulteriori necessità che possano prospettarsi; in tale periodo intermedio tra la fine del rapporto e detto termine, i dati saranno conservati dal Responsabile per fini esclusivamente di sicurezza e non oggetto di ulteriori trattamenti.

Nel caso di risoluzione del contratto ai sensi dell'articolo 8 del presente atto, il Responsabile del trattamento, a scelta del Titolare del trattamento, cancella tutti i dati personali trattati per conto del Titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al Titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto del presente atto.

In caso di richiesta scritta del Titolare, il Responsabile è tenuto a rilasciare un'attestazione scritta dell'avvenuta operazione di cancellazione indicando le modalità tecniche e le procedure utilizzate per la cancellazione.

In deroga a quanto indicato ai punti precedenti, il Responsabile dovrà conservare detti dati nel caso ciò sia previsto dal diritto dell'Unione o dello Stato fino al termine imposto dalla normativa.

ART. 10 – TRASFERIMENTO DEI DATI

Qualunque trasferimento di dati personali da parte del Responsabile del trattamento verso un paese terzo o un'organizzazione internazionale può essere effettuato, nel rispetto del capo V del Regolamento (UE) 2016/679, soltanto previa indicazione e istruzione documentata del Titolare del trattamento.

Il Titolare del trattamento conviene che, qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del Titolare del trattamento) e queste comportino il trasferimento di dati personali ai sensi del capo V del Regolamento (UE) 2016/679, il Responsabile del trattamento e il sub-Responsabile del trattamento possono garantire il rispetto di tale capo V del Regolamento (UE) 2016/679, in particolare utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

ART. 11 - DISPOSIZIONI FINALI

Le parti si danno atto che il presente documento costituisce l'atto di nomina a Responsabile ed ogni sua disposizione è interpretata in modo prevalente rispetto ad ogni altra disposizione eventualmente contrastante e contenuta in altra documentazione sottoscritta tra le parti.

Il mancato rispetto delle disposizioni in materia di trattamento dei dati e delle indicazioni impartite col presente atto costituisce elemento di valutazione per l'eventuale prosecuzione o rinnovo del rapporto sottostante.

La presente nomina non comporta alcun diritto, da parte del Responsabile, ad uno specifico compenso o indennità o rimborso né ad un incremento del compenso previsto per l'erogazione del

servizio.

Le parti si riservano di modificare o integrare il presente atto di nomina nel caso in cui ciò si rendesse necessario.

Per tutto quanto non espressamente previsto, si rinvia alle disposizioni generali vigenti applicabili in materia di protezione dei dati personali.

Letto, confermato e sottoscritto

IL TITOLARE DEL TRATTAMENTO

IRCCS Ospedale Policlinico San Martino

Il Direttore Generale

Dott. Marco Damonte Prioli

Per accettazione

IL RESPONSABILE DEL TRATTAMENTO

Fondazione IRCCS Ca' Granda

Ospedale Maggiore Policlinico

Il Direttore Generale

Dott. Matteo Stocco