ATTO DI DESIGNAZIONE SOGGETTO AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI
ai sensi dell'articolo 29 del Regolamento (UE) 2016/679 (GDPR) e dell'articolo 2-quaterdecies del d.lgs. 196/2003 (Codice Privacy) e ss.mm.ii.

PREMESSO CHE

- il Regolamento (UE) 2016/679 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 (di seguito, "Regolamento"), pone l'accento sulla responsabilizzazione ("accountability") del Titolare e del Responsabile, ossia sull'adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;

- il parere del Autorità Garante per la Protezione dei Dati personali del 12 maggio 2020 sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231, attribuisce ai componenti dell'ODV il ruolo di soggetti autorizzati al trattamento ai sensi degli artt. 29 e 32, paragrafo 4, del Regolamento e dell'art. 2-*quaterdecies* del codice Privacy;

- l'art. 29 del Regolamento dispone che "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

- l'art. 2-quaterdecies del D.lgs. n.196/2003 (Codice Privacy) prevede che "*1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

CONSIDERATO CHE

- in data 22 aprile 2026 l'Ospedale Israelitico (di seguito Ospedale), ai sensi e per gli effetti del D. Lgs. 231/2001, ha nominato quale componente dell'**Organismo di Vigilanza** monocratico l'Avv. Giovanni D'Alessandro;

- in conformità a quanto previsto dal Decreto Legislativo n. 24/2023 (di seguito "Decreto Whistleblowing"), l'Ospedale ha individuato lo stesso Avv. Giovanni D'Alessandro nella sua qualità di Organismo di Vigilanza, quale soggetto incaricato alla Gestione delle segnalazioni in materia di Whistleblowing;

- l'art. 12 del "Decreto Whistleblowing" dispone e che il soggetto individuato formalmente quale gestore delle segnalazioni degli illeciti sia espressamente autorizzato al trattamento ai sensi degli artt. 29 e 32, paragrafo 4, del Regolamento e dell'art. 2-*quaterdecies* del codice Privacy;

- in data 31/6/2026 l'Ospedale ha formalmente attribuito all'Avv. Giovanni D'Alessandro, nella sua qualità di Organismo di Vigilanza, anche la funzione di attestazione degli obblighi di pubblicazione ai sensi del D. Lgs. 33/2013, in quanto l'Ospedale rientra tra gli "enti di diritto privato in controllo pubblico" o "regolati o finanziati" ai sensi dell'art. 2-bis, comma 2 e comma 3, del medesimo decreto, come qualificati dall'ANAC con Delibera n. 1160 del 09/11/2016;

- l'applicazione degli obblighi di trasparenza a tali enti è soggetta al duplice limite di cui all'art. 2-bis, comma 3, ossia "in quanto compatibile" con la natura privatistica dell'ente e "limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse", limite che definisce anche il perimetro dei dati personali trattabili nell'esercizio della funzione di attestazione;

TANTO PREMESSO E CONSIDERATO

L'Ospedale Israelitico, con sede legale in Roma, piazza S. Bartolomeo all'Isola 21 - Cod. Fisc. 80203290582, in qualità di Titolare del Trattamento dei Dati Personali, nella persona del Dr. Anticoli Stefano, in veste di Delegato Privacy, con il presente atto

DESIGNA

L'Avv. Giovanni D'Alessandro, quale persona autorizzata al trattamento dei dati personali ai sensi degli artt. 29 e 32, paragrafo 4 del Regolamento (UE) 2016/679 (GDPR) e dell'articolo 2-*quaterdecies* del d.lgs. 196/2003 (Codice Privacy) e ss.mm.ii, e trasmettendo al designato le seguenti istruzioni a cui dovrà attenersi per ogni attività di trattamento di dati personali effettuata nello svolgimento delle attività specifiche della sua funzione.

1. Trattamenti connessi alla funzione di Organismo di Vigilanza

La presente autorizzazione al trattamento dei dati personali, strutturata ai sensi degli artt. 29 e 32, paragrafo 4, del Regolamento (UE) 2016/679 e dell'art. 2-*quaterdecies* del Dlgs 196/2003, la impegna a trattare i dati personali per la funzione da Lei svolta all'interno dell'Ospedale, come riportato nel "Modello di Organizzazione, Gestione e Controllo" dell'Ospedale Israelitico adottato ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, e la vincola all'obbligo di riservatezza, anche dopo il termine del mandato in essere, in merito alle informazioni trattate e al rispetto della vigente normativa sulla protezione dei dati personali.

L'ambito e le finalità di trattamento dei dati personali connessi all'espletamento delle sue funzioni sono complessivamente definiti dal ruolo da lei ricoperto e specificate nel mandato conferitole ai sensi del d.lgs. 231/2001 (Organo di Vigilanza e Controllo).

Lei potrà quindi trattare esclusivamente i dati personali necessari per adempiere ai compiti connessi al ruolo affidatole e per le basi giuridiche di cui all'art. 6.1c (obbligo legale) e art. 6.1.f (legittimo interesse); a tale scopo, l'Ospedale la autorizza il trattamento in modalità cartacea e automatica e l'accesso alle informazioni contenute nelle banche dati per le operazioni di trattamento pertinenti.

Se nel corso delle sue attività fosse necessario trattare categorie particolari di dati personali ai sensi dell'art. 9 del GDPR e dati personali relativi a condanne penali e reati o a misure di sicurezza ai sensi dell'art. 10 del GDPR, Lei dovrà agire nel rispetto degli art. 9 e 10 del GDPR.

Poiché non si esclude che emergano, nel corso delle attività specifiche del suo ruolo, nuovi trattamenti indotti da modifiche normative che non le devono essere preclusi, i trattamenti di seguito riportati non sono da considerare come esaustivi; lei potrà sempre mettersi in contatto con il Delegato Privacy per modificare l'ambito della sua operatività nel rispetto del presente incarico.

Pertanto, Le si presentano, di seguito, i principali trattamenti a lei delegati come emersi dal Modello Organizzativo adottato dall'Ospedale ai sensi del D. Lgs. 231/2001:

- svolgere periodica attività di audit e di controllo, di carattere continuativo ed anche a sorpresa se ritenuto necessario, in considerazione dei vari settori di intervento e/o delle tipologie di attività e dei loro punti critici per verificare l'efficienza e l'efficacia del Modello.
  Nello svolgimento di tale attività, l'OdV può:
  a) accedere liberamente presso qualsiasi ufficio e unità organizzative dell'Ospedale – senza necessità di alcun avviso e/o consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal Decreto, da tutto il personale dipendente e dirigente;
  b) richiedere informazioni rilevanti o l'esibizione di documenti, anche informatici, inerenti alle attività identificate come sensibili al rischio di commissione di reati, agli amministratori, agli organi di controllo, ai collaboratori, ai consulenti ed in generale a tutti i soggetti tenuti all'osservanza del Modello.
- curare i rapporti e assicurare i flussi informativi di competenza con le unità organizzative e verso gli organi sociali;
- verificare la predisposizione di un efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del Decreto, garantendo la tutela e la riservatezza del segnalante;
- segnalare tempestivamente all'organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo all'Ospedale e proporre le eventuali sanzioni;
- avvalersi del supporto di unità organizzative e strutture interne all'Ospedale con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo;
- supportare le singole aree operative svolgendo funzioni consultive e propositive affinché l'organizzazione si sviluppi nell'ambito e secondo criteri di eticità.

2. Segnalazione di Illeciti – Whistleblowing

Con riferimento in particolare ai compiti a Lei assegnati in materia di gestione delle segnalazioni, come precisati nel documento "Policy Whistleblowing" recante le "Istruzione operativa alla presentazione e gestione delle segnalazioni", Lei si impegna a trattare qualsivoglia dato personale attinente alle segnalazioni di cui dovesse entrare a conoscenza attivando ogni protezione necessaria nel rispetto della normativa vigente.

Ai sensi degli artt. 12 e13 del Decreto Legislativo n. 24 del 2023, Lei dovrà:

- effettuare ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, prevista dal presente decreto, a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51;
- trattare solo quei dati personali strettamente ed oggettivamente necessari per verificare la fondatezza della Segnalazione e procedere alla risoluzione della stessa ai sensi dell'art. 6.1c (obbligo legale) del GDPR. Nel caso venissero raccolti, anche accidentalmente, dati personali manifestamente non necessari per la gestione della Segnalazione, procedere a cancellare immediatamente tali dati;
- agire nei limiti di quanto consentito dalla normativa di cui al Decreto Whistleblowing, e nel rispetto degli art. 9 e 10 del GDPR laddove nel corso delle sue attività fosse necessario trattare categorie particolari di dati personali ai sensi dell'art. 9 del GDPR e dati personali relativi a condanne penali e reati o a misure di sicurezza ai sensi dell'art. 10 del GDPR;
- accertare che i diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 siano esercitati nei limiti di quanto previsto dall'articolo 2-*undecies* del decreto legislativo 30 giugno 2003, n. 196;
- per le segnalazioni ricevute tramite incontro diretto orale (per facoltà del segnalante), somministrare *"Informativa al trattamento dati connessi alle segnalazioni"*, raccogliere il consenso del segnalante e documentare la segnalazione mediante registrazione su dispositivo idoneo o tramite verbale;
- archiviare tutte le segnalazioni ricevute, indipendentemente dal canale utilizzato, per 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;
- assicurarsi che ogni altro soggetto interno che fosse chiamato a collaborare all'istruzione della segnalazione sia stato preventivamente ed espressamente autorizzato al trattamento dati ai sensi ai sensi degli artt. 29 e 32, paragrafo 4 del Regolamento (UE) 2016/679 (GDPR) e dell'articolo 2-quaterdecies del d.lgs. 196/2003 (Codice Privacy) e ss.mm.ii.

3. Misure di sicurezza tecniche e organizzative e accesso alla piattaforma whistleblowing

Ai sensi della Normativa vigente in materia di trattamento dei dati personali, con la sottoscrizione della presente designazione, Lei si impegna a trattare i dati personali, in base all'art. 5 del GPDR, in modo lecito, corretto e trasparente, assicurando che siano:

- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati") e alle sole necessità funzionali in riferimento ai propri compiti da assolvere, rispettando le direttive impartite dal Titolare del Trattamento;
- esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
- adeguatamente protetti da trattamenti non autorizzati o illeciti e da perdite, distruzioni o danni accidentali ("integrità e riservatezza"), rispettando le misure di sicurezza predisposte dal Titolare.

Per la gestione delle segnalazioni degli illeciti, l'Ospedale ha implementato una piattaforma telematica a cui Lei avrà accesso attraverso un sistema di autenticazione personalizzato con nome utente e password, da gestire con cura e diligenza.

Ad ogni modo, nell'effettuare le suddette operazioni di trattamento, Lei si impegna a rispettare le misure di sicurezza fisiche, logiche, ambientali organizzative e informatiche descritte nelle procedure e nelle policies dell'Ospedale, che Lei dichiara di conoscere, avendo cura di proteggere dati e/o applicazioni e/o sistemi utilizzati per il trattamento da ogni forma di accesso abusivo o non consentito da parte di terzi non autorizzati.

3. Bis Attestazione degli obblighi di pubblicazione ex D. Lgs. 33/2013

Con riferimento ai compiti di attestazione degli obblighi di pubblicazione a Lei assegnati, Lei tratterà i dati personali strettamente necessari alla verifica della completezza, dell'aggiornamento e della correttezza dei dati e dei documenti pubblicati nella sezione "Amministrazione Trasparente" dell'Ospedale, sulla base giuridica dell'obbligo legale di cui all'art. 6, paragrafo 1, lett. c) del Regolamento, letto in combinato disposto con l'art. 2-bis, comma 3, del D. Lgs. 33/2013.

Il trattamento è circoscritto, in ragione del richiamato duplice limite normativo, ai soli dati e documenti inerenti all'attività di pubblico interesse svolta dall'Ospedale in virtù dei rapporti convenzionali e di accreditamento con la Pubblica Amministrazione, con esclusione di ogni altro dato relativo all'attività privatistica dell'Ente non riconducibile a tale ambito.

Nello svolgimento di tale attività, Lei potrà:

- accedere alla sezione "Amministrazione Trasparente" e alla relativa documentazione sottostante (compensi, incarichi, curricula, dichiarazioni e ogni altro dato oggetto di pubblicazione obbligatoria) al solo fine di verificarne la conformità agli obblighi di legge;
- richiedere alle unità organizzative competenti la trasmissione dei dati e dei documenti necessari alla predisposizione della griglia di rilevazione e dell'attestazione, nei limiti di cui sopra;
- trattare dati relativi a soggetti terzi (dirigenti, dipendenti, collaboratori) esclusivamente nella misura in cui tali dati siano oggetto di obbligo di pubblicazione, astenendosi da ogni trattamento ulteriore o per finalità diverse.
- Restano ferme, anche per i trattamenti di cui al presente paragrafo, le misure di sicurezza tecniche e organizzative, gli obblighi di riservatezza e le istruzioni generali di cui ai successivi paragrafi del presente atto.

4. Posta elettronica

Per lo svolgimento della sua attività, le è stata assegnata una casella di posta elettronica aziendale sotto il suo completo controllo. La casella di posta è uno strumento di lavoro e Lei è responsabile del suo corretto utilizzo. Le è fatto divieto di utilizzare la posta elettronica aziendale per l'invio o la ricezione di messaggi personali o di messaggi estranei al rapporto esistente tra lei e l'Ospedale.

Le credenziali per l'accesso al sistema di posta elettronica (username e password) devono essere da Lei custodite con attenzione per ridurre i rischi di accesso illecito; la password dovrà essere sostituita con una periodicità non superiore ai tre mesi.

Nel caso avesse notizia di accessi abusivi effettuati da terzi non autorizzati tramite le credenziali a lei assegnate dovrà darne immediata comunicazione al Responsabile dei Sistemi Informativi dell'Ospedale.

5. Documenti cartacei, strumenti informatici utilizzati per il trattamento

Per lo svolgimento della sua funzione, Lei si impegna a rispettare le seguenti istruzioni:

- i dati oggetto di trattamento possono essere trattati soltanto da soggetti appositamente autorizzati e nel rispetto del proprio ambito di trattamento;
- l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
- è vietato raccogliere dati personali diversi da quelli previsti per le finalità specificamente individuate per ciascun autorizzato, o tanto meno utilizzarli per scopi diversi, ancorché connessi alle mansioni svolte in Ospedale, se non a seguito di formale processo di autorizzazione da parte dei propri responsabili;
- durante il trattamento, i documenti devono essere custoditi e controllati in modo che ad essi non accedano persone prive di autorizzazione, in particolare non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

In caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;

- concluso il trattamento, i documenti devono essere collocati in una stanza presidiata dal personale autorizzato o, se la stanza non è presidiata, i documenti devono essere collocati in un armadio dotato di serratura o nella stessa stanza dotata di porta con serratura;
- in occasione della trasmissione dei documenti all'interno ed all'esterno dell'Ente devono essere adottati tutti gli accorgimenti necessari ed idonei ad evitare che le informazioni riservate possano essere lette, sia pure accidentalmente, da chi non è autorizzato (ad esempio mediante trasporto dei documenti in plichi chiusi);
- i documenti riportanti dati personali e particolari non devono essere riciclati onde evitare il rischio che gli stessi possano essere letti da chi non è autorizzato; devono essere eliminati utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, sminuzzati in modo da non essere più ricomponibili;
- raccogliere, registrare e conservare i dati personali raccolti e trattati in maniera informatica avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- è fatto assoluto divieto di estrarre e portare fuori dall'azienda, in copia od in originale, gli archivi, informatici o cartacei, esistenti in azienda, tranne nei casi previsti e concordati con il proprio responsabile, che devono essere di volta in volta definiti;
- per l'accesso ai sistemi informatizzati utilizzare password riservata e personalizzata;
- la password non deve essere composta da riferimenti agevolmente riconducibili alla propria persona (ad esempio nome, cognome, data di nascita, nome del coniuge); non deve essere trascritta su promemoria in vista (ad esempio biglietti dinanzi al pc o affissi in bacheca) o comunicata a terzi;
- non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento, non lasciare il PC con l'utenza abilitata per impedirne l'utilizzo fraudolento, non lasciare in vista le informazioni presenti sul monitor. Alla fine del lavoro scollegarsi dal PC.
- non installare e non scaricare da Internet programmi non pertinenti l'attività lavorativa né qualsiasi altro programma, senza la preventiva autorizzazione da parte del Responsabile dei Sistemi Informativi aziendali;
- comunicare tempestivamente al Responsabile dei Sistemi Informativi, l'eventuale rilevazione di anomalie nell'utilizzo del sistema informatico che possono compromettere la sicurezza dei dati;
- verificare la provenienza dei messaggi di posta elettronica contenenti allegati; e cancellare direttamente quelli di dubbia provenienza;
- utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- non diffondere messaggi di posta elettronica (es: catena di S. Antonio).

In caso di furto o smarrimento degli strumenti di lavoro utilizzati per lo svolgimento delle attività dovrà darne immediata comunicazione al Responsabile dei Sistemi Informativi dell'Ospedale, eventualmente allegando alla stessa copia della denuncia di furto alle autorità competenti.

6. Conclusione del rapporto contrattuale

Qualora, per qualunque motivo, venisse meno o perdesse efficacia il rapporto giuridico tra lei e l'Ospedale, la presente autorizzazione decadrà automaticamente meno senza bisogno di specifiche comunicazioni o revoche.

Ad ogni modo, si ricorda che gli obblighi relativi alla riservatezza dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

7. Rispetto degli obblighi assunti in merito al trattamento di dati personali

Resta inteso che il presente documento e le istruzioni in esso contenute non comportano alcun diritto ad uno specifico compenso e/o indennità e/o qualifica derivante dagli obblighi di questo documento.

La preghiamo di controfirmare la presente autorizzazione, che sarà depositata agli atti, per presa visione e accettazione.

Roma, lì 31/6/2026

Per il Titolare del Trattamento

Il Delegato Privacy

Per accettazione

L'OdV

Giovanni D'Alessandro