ATTO DI NOMINA DEL SOGGETTO DESIGNATO AL TRATTAMENTO DEI DATI PERSONALI

- Richiamati il Regolamento (UE) 2016/679 del Parlamento del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR o Regolamento) e il D.Lgs. 30 giugno 2003, n° 196: *"Codice in materia di protezione dei dati personali"* come novellato dal D. Lgs. 10 agosto 2018, n° 101;

- Rilevato che il l'art. 2-quaterdecies del D.Lgs. 196/2003 conferisce in capo al Titolare o al Responsabile, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, la possibilità di attribuire a persone fisiche espressamente designate, che operano sotto la propria autorità diretta, specifici compiti e funzioni connessi al trattamento di dati personali;

- Ritenuto, anche in considerazione della complessità dell'organizzazione interna di un'Azienda Ospedaliera, che l'attribuzione di specifici compiti e funzioni relativi al trattamento dei dati personali, a persone fisiche ("*Designati al Trattamento*") consente di intervenire in maniera strategica alla corretta gestione della privacy, nonché di presidiare il *"Sistema Privacy";*

- Dato atto che nel rispetto della normativa ante Regolamento UE 679/2016, l'AOU San Luigi Gonzaga di Orbassano in qualità di Titolare del trattamento aveva individuato e nominato i Responsabili interni al trattamento dei dati;

- Rilevata l'opportunità, in continuità rispetto alle scelte organizzative assunte negli anni dall'Azienda, di adottare un modello organizzativo che faciliti l'assolvimento dei compiti di natura organizzativa, documentale e tecnica in materia di protezione dei dati personali;

- Considerato che l'art. 32, paragrafo 4, del GDPR prevede che "il Titolare del trattamento e il Responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

- Dato atto che il Soggetto Designato al trattamento risponde direttamente in caso di eventuali violazioni derivanti da una sua condotta illecita o scorretta o in contrasto con i principi del GDPR o con le istruzioni impartite dal Titolare;

- Richiamata la deliberazione n. ..... del..... con la quale sono stati individuati i soggetti designati del trattamento dei dati;

- Dato atto che Titolare del Trattamento è l'Azienda Universitaria Ospedaliera nel suo complesso

- Dato atto che i poteri organizzativi sono in capo al Direttore Generale pro tempore (eventualmente al Commissario Straordinario o al Direttore facente funzioni) e che a esso sono attribuiti anche la rappresentanza legale dell'Ente

L'AOU San Luigi Gonzaga di Orbassano, con sede legale in Orbassano, Regione Gonzole 10, C.F. 95501020010 e P. IVA 02698540016, in qualità di Titolare del Trattamento dei dati personali, nella persona del Legale Rappresentante, con il presente atto

in considerazione della Sua esperienza, capacità ed affidabilità.

NOMINA
SOGGETTO DESIGNATO AL TRATTAMENTO DEI DATI

Il dott/la dott.ssa _____, in

qualità di _____

La nomina di soggetto designato è strettamente correlata all'incarico conferitoLe, non è delegabile e decade per Sue dimissioni/cessazione dal servizio, o per revoca che può essere disposta in qualsiasi momento dal Titolare, anche senza preavviso.

Tale nomina non prevede alcuna remunerazione aggiuntiva

Della presente nomina si darà evidenza mediante pubblicazione dell'elenco dei nominativi dei delegati nella specifica sezione del sito istituzionale.

COMPITI E LE RESPONSABILITA' DEL SOGGETTO DESIGNATO

PRINCIPI GENERALI DA OSSERVARE

Il Soggetto Designato deve:

- effettuare il trattamento dei dati nel rispetto della normativa vigente in materia di privacy, pubblicità e trasparenza della P.A.;

- effettuare il trattamento dei dati personali attenendosi alle disposizioni previste dalla normativa e alle procedure e istruzioni impartite dal Titolare, provvedendo **all'organizzazione, alla gestione, nonchè alla supervisione** di tutte le operazioni di trattamento gestiti nell'ambito della propria struttura e della funzione ricoperta;

- provvedere all'espletamento di tutte le operazioni necessarie al fine di garantire il rispetto dei Principi applicabili al trattamento dei dati, ai sensi dell'art. 5 del GDPOR, ed in particolare dei principi di **liceità, correttezza e trasparenza,** nonché:

a. del principio di **MINIMIZZAZIONE** dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità di trattamento;
b. del principio di **LIMITAZIONE** delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
c. del principio di **ESATTEZZA**: garantire l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono raccolti e successivamente trattati;

- accertarsi che non vi siano trasferimenti di dati personali al di fuori dello SEE (Spazio Economico Europeo) ove non esista una base di liceità secondo gli articoli da 44 a 49 del GDPR;

- adoperarsi con il supporto della Commissione Aziendale Privacy e del DPO, al fine di garantire ex art. 25 del GDPR l'applicazione del principio di "*privacy by design & privacy by default*", per effettuare una valutazione della **Compliance al GDPR** dei sistemi e applicazioni sviluppati prima del 25 maggio 2018 e, se necessario, richiederne l'aggiornamento, nonché per i nuovi trattamenti (es. sperimentazioni cliniche);

- mantenere la **riservatezza** rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti assegnati, e osservare gli obblighi di legge in materia di comunicazione e diffusione dei dati personali, anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro;

- assicurare l'osservanza delle istruzioni impartite da altro Titolare, quando l'Azienda agisce in qualità di Responsabile del Trattamento;

- partecipare direttamente alle iniziative formative per promuovere e sviluppare a cultura della protezione e sicurezza del dato;

- collaborare con il Direttore Generale/Commissione Aziendale Privacy per l'adozione delle modalità più idonee al trattamento dei dati;

- collaborare tempestivamente con il Direttore Generale/Commissione Aziendale Privacy/ DPO nel caso di eventuali ispezioni e violazioni dei dati;

- supportare il Titolare in caso di indagini giudiziarie, ispezioni o AUDIT interni;

- informare prontamente il Direttore Generale/Commissione Aziendale Privacy di tutte le comportamenti/questioni rilevanti ai fini di legge e/o eventuali problematiche che costituiscono un rischio per la protezione dei dati personal;

- prestare la più ampia e completa collaborazione al DPO al fine di compiere tutto quanto sia necessario e opportuno in relazione agli adempimenti imposti dalla normativa in materia di trattamento di dati personali, fornendo allo stesso, su richiesta e secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo.

La violazione delle presente istruzioni può comportare l'irrogazione di sanzioni disciplinari e il corretto adempimento delle stesse può fare parte della valutazione delle performance. Il Designato è considerato nel contempo anche Autorizzato e pertanto deve seguire le relative istruzioni per quanto compatibili.

COMPITI PARTICOLARI DEL DESIGNATO

Con riferimento al personale operante nella Struttura:

Il Soggetto Designato deve:

- **individuare** e **nominare per iscritto**, quali **autorizzati**, secondo le rispettive competenze, i soggetti che svolgono operazioni di trattamento all'interno della Struttura di propria competenza (dipendenti, collaboratori, specializzandi, stagisti, frequentatori, ecc.), fornendo loro specifiche istruzioni operative riguardanti le operazioni di raccolta, trattamento e archiviazione dei dati personali su supporto informatico e cartaceo e individuando l'ambito di trattamento consentito. (La documentazione relativa alla nomina è disponibile sulla Intranet aziendale nella sezione Privacy – comunicazioni operative-Soggetti autorizzati);

- **aggiornare** periodicamente **l'elenco degli autorizzati**;

- **diffondere** agli autorizzati le **direttive, le procedure aziendali e/o circolari interne** in materia fornite dal Titolare;

- **attenersi** alle indicazioni fornite per la creazione dei **codici identificativi personali e le password** per il trattamento dei dati effettuato con sistemi automatizzati/ accesso a piattaforme aziendali da consegnare agli autorizzati, vigilando sul corretto uso degli stessi, segnalando immediatamente ai Sistemi Informativi Informatici eventuali dimissioni/cessazioni del personale, in modo da consentire la disattivazione delle credenziali rilasciate;

- **vigilare sul rispetto delle istruzioni impartite** agli autorizzati e garantire che il trattamento dei dati avvenga in modo lecito e corretto, nel rispetto dei principi di cui all'art. 5 del GDPR e del D. Lgs. 196/2003 e s.m.i;

- **vigilare sul rispetto delle misure di sicurezza** da parte del personale autorizzato, al fine di evitare rischi, anche accidentali, di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di trattamento;

- **verificare l'applicazione**, da parte degli autorizzati, **delle indicazioni fornite dal Titolare** per una corretta trasmissione dei documenti con particolare attenzione a quelli contenenti dati sanitari e/o appartenenti a particolari categorie di dati all'interno e all'esterno dell'Azienda. In particolare tutta la documentazione cartacea contenente tali dati deve essere

obbligatoriamente protetta e consegnata ai vari servizi dell'Azienda in modo tale che i dati dell'interessato non siano visibili (es. busta chiusa). I referti diagnostici e ogni altra documentazione sanitaria possono essere ritirati anche da persone diverse dai diretti interessati purchè munite di delega scritta e con consegna in busta chiusa sulla quale deve essere apposto il timbro "*Da aprirsi a cura dell'interessato*. L'invio di tali dati via e-mail non può avvenire in "chiaro", ma occorre renderlo "sicuro" attraverso la creazione di un file compresso (7zip o altri strumenti analoghi disponibili sul proprio PC) protetto da password (*Circolare prot. n.2676 del 17.02.2020-disponibile sulla Intranet aziendale*);

- **sensibilizzare il personale** in materia di protezione dei dati, collaborando alla redazione del piano di formazione aziendale, fornendo al Direttore Generale/Commissione Aziendale Privacy il fabbisogno formativo della propria struttura e promuovendo e garantendo la partecipazione del personale autorizzato agli eventi formativi organizzati al riguardo dall'Azienda;

- **individuare all'interno della Struttura**, in qualità di **referente**, un professionista particolarmente motivato e sensibile alla materia, con il compito di mantenere i contatti e collaborare con la Commissione Aziendale Privacy e il DPO, n verificare periodicamente i contenuti dell'applicativo aziendale che gestisce il Registro informatizzato dei trattamenti;

- **comunicare** immediatamente ai **Sistemi Informativi Informatici** la **dimissione/cessazione di un soggetto autorizzato o la revoca delle autorizzazioni** al trattamento dei dati, al fine di consentire la disattivazione dell'accesso al sistema per i soggetti in questione.

Con riferimento alle operazioni di trattamento dei dati:

Il Soggetto Designato deve:

- attenersi scrupolosamente alle disposizioni previste dal GDPR e alle conseguenti procedure e istruzioni emanate in materia di privacy dal Titolare del trattamento, garantendo, anche con **verifiche periodiche**, per ciascun trattamento di propria competenza il rispetto dei principi di ordine generale previsti dalla normativa vigente e in particolare che i dati siano esatti, aggiornati e completi;

- attenersi alle specifiche istruzioni fornite dal Comitato Europeo per la Protezione dei dati e dall'Autorità Garante per particolari trattamenti (videosorveglianza, dossier sanitario, fascicolo sanitario, referti on line, ricerca scientifica, trattamento di dati genetici, trattamento dei dati nell'ambito del rapporto di lavoro, Linee guida su internet e posta elettronica, ect.), verificandone il puntuale rispetto;

- **individuare per ogni trattamento**, con il supporto della Commissione Aziendale Privacy e del DPO, **le finalità e la base di liceità** in riferimento all'art. 6 del GDPR, tra obbligo legale, pubblico interesse, salvaguardia degli interessi vitali dell'interessato, contratto con l'interessato, consenso libero dell'interessato, e art. 9 par. 2 del GDPR tra finalità di medicina, prevenzione sanitaria, tutela dell'interesse vitale dell'interessato, ricerca scientifica, necessità per il diritto del lavoro e sicurezza sociale, consenso dell'interessato. Qualora il trattamento di categorie particolari di dati sia effettuato per motivi di interesse pubblico rilevante è necessario indicare una delle previsioni di cui all'art. 2 sexies del D.Lgs.

196/2003 s.m.i. In caso di dati giudiziari deve essere applicato l'art. 2 octies. Costituisce base di liceità il rispetto dei Codici Deontologici per trattamenti per scopi statistici e scientifici, per quelli a fini statistici e di ricerca scientifica nell'ambito del SISTAN, per quelli a fini di archiviazione nel pubblico interesse o di ricerca storica e per quelli effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;

- **conformare,** con il supporto della Commissione Aziendale Privacy e del DPO, i trattamenti alle Autorizzazioni Generali del Garante e altri suoi provvedimenti applicabili,

- **assicurarsi che i dati da pubblicare sul sito istituzionale siano conformi** alla normativa in materia e siano rispettati gli **obblighi di trasparenza e tracciabilità**. Si ricorda che è **assolutamente vietata la pubblicazione/diffusione di dati sanitari/particolari categorie di dati anche in forma pseudonimizzata** cioè anche con la pubblicazione delle sole iniziali o altri codici che potrebbero insieme ad altre informazioni permettere l'identificazione dell'interessato;

- garantire **la conservazione dei dati** in una forma che consenta l'identificazione degli interessati per un **periodo di tempo non superiore al conseguimento delle finalità** per le quali sono trattati;

- **distruggere i dati personali** in caso di **cessazione del trattamento,** o al **termine del periodo di conservazione**, nel rispetto di quanto previsto in merito dalla normativa e dalle procedure aziendali (*Regolamento per l'archivio e la conservazione degli atti*- disponibile sulla Intranet aziendale Sezione Affari Generali – Regolamenti e Procedure);

- effettuare, sia per i trattamenti in essere sia per i nuovi trattamenti in fase di progettazione, ove necessaria, una **valutazione di impatto** conforme alle direttive stabilite nel Regolamento Generale sulla protezione dei dati personali n. 679/2016, e ai Provvedimenti dell'Autorità di controllo. (In particolare le *"Guidelines on Data Protection Impact Assessment (DPIA)"* (wp248), nonché l'*'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati"* ai sensi dell'art. 35, paragrafo 4, del Regolamento (UE) n. 2016/679). In tali casi il Designato del trattamento dati personali deve coinvolgere il DPO;

- **collaborare** con il Direttore Generale/Commissione Privacy, anche per il tramite del referente privacy individuato all'interno della Struttura, nella **compilazione e continuo aggiornamento del Registro informatizzato dei trattamenti** attraverso:
    - la **redazione e l'aggiornamento periodico** dell'elenco delle tipologie dei dati trattati nell'ambito della Struttura di competenza, dando comunicazione scritta alla Commissione Aziendale Privacy di ogni variazione (anche nel caso di passaggio dalla modalità cartacea a quella elettronica) e/o introduzione di nuovi trattamenti;
    - la **comunicazione** alla Commissione Aziendale Privacy e al DPO delle **modifiche** relative alle attività di trattamento dei dati, nonché gli eventuali **cambiamenti organizzativi o tecnici** che possano incidere direttamente sugli stessi (es. acquisizione di nuove banche dati e/o applicativi hardware, etc.);

- provvedere alle incombenze previste in **caso di cessazione del trattamento** di dati personali secondo le formalità di legge, informandone la Commissione Aziendale Privacy e il DPO;

- individuare, in caso di esternalizzazione di trattamenti, le modalità di condivisione dei dati personali e assicurare la liceità della trasmissione degli stessi (per norma oppure riconducendolo alle previsioni dell'art. 26 del GDPR: Contitolare e dell'art. 28 del GDPR:Responsabile;

- qualora il designato rivesta il ruolo di RUP /DEC, provvedere **alla nomina dei soggetti esterni quali Responsabili del Trattamento** in relazione all'affidamento agli stessi di determinate attività effettuate per conto del Titolare,(art. 28 GDPR- *Bozza standard di accordo disponibile sulla Intranet aziendale* – sezione Privacy-), **verificando,** anche con l'ausilio del DPO e della Commissione Aziendale Privacy, che i Responsabili del trattamento ex art. 28 del GDPR rispettino le istruzioni impartite provvedendo a proporre l'adozione di diverse/ulteriori misure di sicurezza in funzione dello stato dell'arte e di eventuali incidenti di sicurezza. E' necessario dare evidenza dei Responsabili attraverso l'inserimento dei dati necessari sul Registro Informatizzato dei Trattamenti.

Con riferimento alle misure di sicurezza

Il Soggetto Designato deve:

- **attenersi alle misure di sicurezza tecniche e organizzative** previste dalle normativa vigente (es. Misure Minime ICT AGID, misure previste dal piano di sicurezza cibernetica nazionale) e dai provvedimenti del Garante, nonché eventuali misure ritenute idonee individuate dal Titolare atte a preservare la disponibilità ed integrità dei dati trattati;

- adottare le misure necessarie affinchè **i dati trattati** siano **custoditi in locali protetti**, verificando periodicamente le modalità di accesso ai locali e/o archivi ai soli soggetti autorizzati (le persone ammesse in uffici e locali contenenti particolari categorie di dati (es. dati sanitari) a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate). In particolare custodire **la documentazione sanitaria in locali chiusi**, dotati di serratura, sui quali deve essere apposta la scritta con la dicitura:*"ACCESSO RISERVATO AL PERSONALE AUTORIZZATO*;

- custodire e conservare adeguatamente **i supporti utilizzati** per le copie dei dati;

- custodire i **monitor e le apparecchiature informatiche**, comprese quelle del sistema di videosorveglianza;

- supportare il Titolare, la Commissione Aziendale Privacy e il DPO **nell'analisi del rischio fisico, informatico e organizzativo**;

- non **esporre le ragioni di assenza del personale ai colleghi**, indicando, se necessario, se il soggetto è richiamabile o meno in servizio;

- **attivare tempestivamente la procedura di data breach** in occasione di qualsiasi incidente/evento che possa compromettere il corretto trattamento e la sicurezza dei dati

(anomalie, furti, perdite accidentali, distruzioni dei dati, indisponibilità prolungata dei dati che compromette il servizio, ecc..) e, in coordinamento con le altre strutture competenti (es. Sistemi Informativi), individuare ed attuare opportune disposizioni per minimizzare l'impatto sui diritti e libertà delle persone fisiche (*Procedura disponibile sulla Intranet Aziendale- Sezione Privacy-Data Breach*);

- **informare** prontamente il Titolare, la Commissione Aziendale Privacy e il DPO di ogni **evento che possa costituire un potenziale pericolo** per i dati personali.

Con riferimento ai diritti degli interessati

Il Soggetto Designato deve:

- provvedere a che **vengano fornite le informazioni di cui agli artt. 13 e 14 del GDPR ai soggetti interessati** ogniqualvolta si raccolgano dati personali, anche avendo cura di affiggere i cartelli contenenti le informative in tutti i locali accessibili al pubblico (D*ocumenti reperibili sulla Intranet Aziendale- sezione Privacy- Informative*);

- nel caso di **trattamenti specifici**, proporre al Titolare, tramite la Commissione Aziendale Privacy, e al DPO l'integrazione delle informazioni e degli eventuali moduli di consenso;

- **raccogliere,** dopo aver fornito l'informativa e **ove necessario, il consenso** espresso dai pazienti quando necessario mediante la compilazione dell'apposito modulo che dovrà essere obbligatoriamente inserito nella cartella clinica degli stessi (*Documento reperibile sulla Intranet aziendale- sezione Privacy- Infor)*;

- attenersi alle procedure aziendali, mettendo in atto le soluzioni organizzative e procedurali più appropriare al fine di garantire e agevolare l'effettivo esercizio del diritto d'accesso e degli altri diritti dell'interessato, di cui al capo III del Regolamento Europeo.

Orbassano, _____

Il Titolare del Trattamento

_____

Il Soggetto designato

_____

Una copia del presente atto di designazione, debitamente firmata, viene restituita al Titolare, c/o la S.S. SAAS