NOMINA DEI RESPONSABILI ESTERNI

Procedura GDPR

Autore/i: DPO
Rivisto da UOC Privacy, Trasparenza e Integrità
Accettato da: Direzione Generale

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1	21/05/2019	Prima versione	U.O.C. / Supporto specialistico
2	08/07/2021	Aggiornamento Procedura	DPO
3	03/01/2023	Aggiornamento Procedura	DPO
4	11/09/2023	Adeguamento alle SCC (Clausole contrattuali standard)	DPO
L'ultima revisione sostituisce qualsiasi revisione precedente.			

A.O.R.N.
Azienda Ospedaliera dei Colli

PROCEDURA PER LA NOMINA DEI RESPONSABILI ESTERNI

Sommario

PREMESSA

Il Regolamento Europeo Generale sulla Protezione dei Dati UE/679/2016 (d'ora in poi GDPR) del 27 aprile 2016, direttamente applicabile in ciascuno degli Stati membri a decorrere dal 25 maggio 2018, stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché norme relative alla libera circolazione di tali dati.Il D.lgs. n. 101 del 10 agosto 2018 reca disposizioni per l'adeguamento della normativa nazionale al GDPR.

Il GDPR ha di fatto cambiato la prospettiva dell'approccio alla tutela della privacy rispetto al Codice Privacy approvato con D.lgs. n. 196/2003, introducendo il principio della responsabilizzazione (*accountability*) per il quale il Titolare deve adottare misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato in conformità alle disposizioni del GDPR medesimo.

CAPITOLO 1
AMBITO DI APPLICAZIONE

CAP. 1

FINALITÀ DEL DOCUMENTO

Con la presente procedura l'Azienda intende disciplinare le modalità operative interne per la ricognizione, identificazione e formale nomina dei "Responsabili esterni al trattamento dei dati" ai sensi del GDPR n. 679/2016, atteso che i trattamenti dati da parte di ciascun Responsabile esterno del trattamento dei dati e le relative connesse responsabilità saranno compiutamente disciplinati da allegato apposito contratto, in conformità al comma 3 dell'art. 28 del GDPR.

La procedura aziendale per la nomina dei Responsabili esterni al trattamento dei dati stabilisce:

- I principi, il processo, le competenze e le responsabilità per l'individuazione, la nomina dei suddetti responsabili e la stipula del contratto;
- I contenuti contrattuali puntuali e specifici che devono connotare gli accordi tra ogni data controller (l'Azienda o ente pubblico titolare del trattamento), che intende esternalizzare un trattamento di dati personali, ed ildata processor incaricato di detto trattamento (fornitore di servizi o di attività/prestazioni esternalizzati, sia esso un outsourcer tradizionale o un cloud service provider).

È, pertanto, necessario tener conto delle indicazioni della procedura in parola già durante le negoziazioni relative a servizi, attività o prestazioni esternalizzati a far data dall'approvazione e, quindi, dall'entrata in vigore della stessa. Contestualmente è necessario, altresì, verificare aggiornare ed integrare i contratti già in essere che comportano esternalizzazione del trattamento di dati personali o parte di esso.

ENTRATA IN VIGORE

Questo documento risulta applicabile non appena viene pubblicato.

SUPPORTO FORNITO DAL DPO

Si specifica che, all'interno della presente procedura, il "supporto" fornito dal DPO della A.O.R.N. Azienda Ospedaliera dei Colli, è di tipo tecnico, attesa la necessaria conoscenza specialistica della normativa e delle prassi in materia di protezione dati, al fine di assolvere i compiti previsti dall'art. 39 del GDPR. Il DPO, infatti, non può in alcun caso prendere decisioni al posto del Titolare del trattamento o sostituirsi nelle valutazioni rimesse dalla normativa data protection in capo a quest'ultimo.

CAPITOLO 2
DEFINIZIONI E NORME DI RIFERIMENTO

❖ ACRONIMI E ABBREVIAZIONI

DPO	Data ProtectionOfficer – Responsabile della Protezione dei Dati
EDPB	European Data Protection Board – Comitato europeo per la Protezione dei Dati. Organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del GDPR.
ENISA	European Union Agency for Network and Information Security
GDPR	General Data ProtectionRegulation – Regolamento Generale sulla Protezione dei Dati, n. 2016/679
IT	Information Technology
WP29	Working Group 29: gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE. Dal 25 Maggio 2018 prende il nome di European Data Protection Board.

❖ DEFINIZIONI

Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, n. 6, GDPR).
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità dell'utente.
Autorità Garante per la Protezione dei Dati Personali	Autorità istituita dalla legge 31 dicembre 1996, n. 675. Ha sede a Roma.
Banca dati	Qualsiasi complesso organizzato di dati (archivio informatico), riguardanti uno stesso argomento o più argomenti correlati tra loro, strutturato in modo tale da consentire la gestione dei dati stessi (l'inserimento, la ricerca, la cancellazione ed il loro aggiornamento) da parte di un applicazione, ripartito in uno o più elaboratori elettronici (ad es. server, postazioni lavorative, ecc.) dislocati all'interno della rete LAN del Titolare.
Cancellazione sicura	Modalità di cancellazione che consiste nell'eliminazione irreversibile dei dati contenuti in un supporto elettronico in modo che essi non siano più accessibili a terzi o risultino comunque inintelligibili impedendo così il recupero degli stessi.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, c. 1, GDPR).
Classificazione	L'attribuzione all'informazione di un livello di classificazione ovvero il suo inserimento all'interno di una classe di sicurezza.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento (art. 4, n. 11, GDPR).
Credenziali di autenticazione	I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati personali relativi a condanne penali o reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR).
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1, GDPR).
Declassificazione	La soppressione di qualsiasi menzione di classificazione.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Documento cartaceo	L'insieme aggregato di informazioni su supporti cartacei.
Documento elettronico	L'insieme aggregato di informazioni su supporti informatici, ovvero file generati attraverso l'utilizzo delle applicazioni informatiche del Titolare.
Incaricato del trattamento	Persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Informazione	La rappresentazione di dati, atti o fatti rilevanti per il Titolare.
Interessato del trattamento	Persona fisica cui si riferiscono i dati personali.
Minimizzazione dei dati	Ogni Titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, nel rispetto dei principi di adeguatezza (proporzionalità rispetto alle finalità) e pertinenza dei dati e limitazione dei trattamenti solo per il raggiungimento delle finalità previste.
Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (art. 4, n. 5, GDPR).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, n. 8, GDPR).
Riclassificazione	La ridefinizione del livello di classificazione attribuito all'informazione e, quindi, lo spostamento all'interno di un'altra classe di sicurezza.
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Sistema informativo	L'insieme di dispositivi, programmi ed infrastruttura di rete.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, n. 7, GDPR).
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, n. 2, GDPR).
Videosorveglianza	Sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate.
Violazione dei dati personali	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, n. 12, GDPR).

❖ NORMATIVA DI RIFERIMENTO

D.lgs. n. 101/2018	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).
D.lgs. n. 196/2003	Decreto Legislativo n. 196 del 30 giugno 2003, contenente il "Codice in materia di protezione dei dati personali", n. c. "Codice Privacdella y".
Regolamento UE 2016/679	Regolamento del Parlamento Europeo e 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021	Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021, relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio
Legge n. 300/1970	Statuto dei Lavoratori.
Provvedimento n. 467/2018	Provvedimento dell'Autorità Garante della Protezione dei Dati Personali n. 467 dell'11 ottobre 2018: "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679".

CAP. 3

CAPITOLO 3
GESTIONE DEI RAPPORTI TRA IL TITOLARE ED I RESPONSABILI ESTERNI DEL TRATTAMENTO

❖ IL RESPONSABILE ESTERNO DEL TRATTAMENTO

Il Responsabile del trattamento dati o "*data processor*", come definito in generale dall'art. 4 comma 1 n. 8 delGDPR n. 679/2016, è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

L'art. 28, in particolare, dispone quanto segue: "*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. Il responsabile del trattamento non ricorre ad altro responsabile senza previa autorizzazione scritta, specifica generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento 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…*".

Quando l'A.O. dei Colli, Titolare del trattamento dei dati o "data controller", ricorre a soggetti esterni (persone fisiche o giuridiche, pubbliche o private, o altri organismi) che forniscono servizi, attività o prestazioni, a qualsiasi titolo, per i quali trattano dati personali/particolari, il "data processor", incaricato di detto trattamento, assume la funzione di Responsabile esterno del Trattamento ai sensi del precitato art 4 co.1 n. 8 e dell'art. 28 del GDPR. Il Responsabile esterno del trattamento dati deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali.

In conformità a quanto disposto dal citato art. 28 GDPR, il Responsabile deve offrire all'A.O. dei Colli garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti stabiliti dalla normativa europea e garantire la tutela dei diritti dell'interessato.

In particolare ciascun Responsabile esterno del trattamento che l'A.O. dei Colli intende nominare, per l'ambito delle funzioni e competenze previste dal sevizio, attività o prestazione oggetto dell'incarico affidatogli, deve possedere specifici 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.

I trattamenti da parte di ciascun Responsabile esterno dell'A.O. dei Colli devono essere definiti da un contratto/accordo a norma del diritto dell'Unione o degli Stati membri, secondo lo schema contrattuale allegato alla presente procedura quale parte integrante e sostanziale, che lo vincoli all' Azienda, Titolare del trattamento, e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità dello stesso, il tipo di dati personali e le categorie di interessati trattati, gli obblighi e i diritti del Titolare del trattamento.

- In conformità a quanto stabilito all'art. 28, commi 3 del GDPR, l'accordo/contratto vincolante tra l'A.O. dei Colli, Titolare del trattamento dei dati, ed il Responsabile esterno del trattamento deve prevedere in particolare a carico di quest'ultimo i seguenti obblighi:
- trattare i dati solo in conformità alle istruzioni — che dovranno essere adeguatamente documentate — ricevute dal titolare; anche in ipotesi di trasferimento dei dati al di fuori dell'Unione Europea;

- garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge;
- Adottare le misure richieste ai sensi dell'art. 32 del Regolamento Europeo, ovvero le misure tecniche e organizzative a protezione dei dati ritenute idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento;
- richiedere, in caso di ricorso al subappalto, una previa autorizzazione scritta da parte del Titolare.

Altri doveri in capo al Responsabile esterno sono:

- rispondere direttamente nei confronti del titolare per eventuali inadempimenti della propria catena di subfornitura;
- informare il titolare, qualora abbia ricevuto un'autorizzazione generale al subappalto, di eventuali variazioni in ordine alla modifica o alla sostituzione di taluno dei propri subappaltatori, dando così l'opportunità al titolare di opporsi a tali modifiche;
- assistere il titolare, mediante misure tecniche e organizzative adeguate fornendo supporto anche alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione);
- assicurare protezione ai dati attraverso misure tecniche e organizzative adeguate, ai sensi dell'art. 32 del GDPR;
- effettuare la valutazione d'impatto (*impact assesment*) richiesta dall'art. 35 del GDPR;
- consultare l'Autorità, qualora la valutazione d'impatto effettuata indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
- cancellare o restituire i dati, su scelta del titolare, al momento della cessazione del rapporto, salvo che la legge non imponga specifici obblighi di conservazione;
- mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente elenco;
- consentire al titolare di effettuare attività di audit, direttamente o per il tramite di terze parti all'uopo incaricate.

❖ STIPULA/REVISIONE DEI CONTRATTI CON I RESPONSABILI ESTERNI TRATTAMENTO DATI (EX ART 28 GDPR)

Il Ruolo di Responsabile Esterno, specificandone i dati identificativi, le funzioni e competenze previste dall'incarico di affidamento del sevizio, attività o prestazione, con riferimento alle connesse operazioni di trattamento dei dati, va formalizzato, a norma dell'art. 28 del Regolamento UE 679/2016, mediante sottoscrizione di apposito contratto redatto secondo lo schema allegato (**all. 1**), salvo eventuali casi specifici che verranno di volta in volta definiti, tenendo conto della natura e della finalità dei dati trattati. Inoltre, nel caso di ricorso da parte del Responsabile ad altri Responsabili (Sub-Responsabili), allegato al suddetto schema di contratto, è prevista **l'Autorizzazione Generale del Titolare alla nomina di Sub-Responsabili del trattamento dei dati personali**.

Nell'ottica di agevolare la identificazione dei soggetti da nominare quali Responsabili esterni del trattamento dati, in allegato (**all. 2**), a titolo indicativo e non esaustivo, si riporta un elenco di servizi, attività e forniture per le quali si rende necessario procedere a tale nomina.

Ciò premesso, è necessario, in applicazione dell'art. 28 del Regolamento UE 679/2016, procedere all'aggiornamento, integrazione o regolarizzazione del ruolo di Responsabile esterno dei soggetti (persone fisiche o giuridiche), che in base a contratti/convenzioni con l'A.O. dei Colli relativi ad attività, prestazioni o servizi, effettuano o effettueranno operazioni di trattamento e/o elaborazione dei dati personali/particolari per conto del Titolare.

In via preliminare si precisa che i Delegati interni al trattamento dati (Direttori UU.OO.CC. e UU.OO.SS.DD., nonché altri soggetti formalmente individuati per la natura e tipologia di dati trattati) sono tenuti a collaborare, per la ricognizione, nonché per il monitoraggio e successivo aggiornamento, di tutti i contratti/convenzioni in essere, o che verranno posti in essere, tra l'A.O. dei Colli e soggetti (persone fisiche o giuridiche) esterni aventi ad oggetto attività, prestazioni o servizi che comportano operazioni di trattamento e/o elaborazione dei dati personali/particolari, supportando il Titolare del trattamento nella relativa nomina. Nello specifico sono infatti tenuti a comunicare al Titolare, al DPO all'UOC Privacy – Trasparenza e Integrità, ogni modifica dell'attività di trattamento dei dati, nonché eventuali mutamenti organizzativi o tecnici (es. acquisizione/trasferimento di banche dati, esternalizzazione di servizi) che possono incidere sugli stessi.

Per l'individuazione e la nomina dei Responsabili, si precisa, nel dettaglio quanto segue.

1) Per i contratti relativi a prestazioni, servizi o forniture che implicano trattamento dati, compete alla **UOC Provveditorato - Economato** trasmettere, tempestivamente, alla UOC Privacy – Trasparenza e Integrità, il provvedimento di aggiudicazione definitiva (delibera/determina) affinché quest'ultima possa procedere alla redazione del suddetto contratto per la formalizzazione del ruolo di Responsabile ex art. 28 GDPR dell'aggiudicatario. Il suddetto provvedimento di aggiudicazione verrà inviato alla UOC Privacy – Trasparenza e Integrità mediante la procedura informatica Lapis-Web.
2) Per le apparecchiature elettromedicali compete alla **UOC Ingegneria Clinica – HTA- SIA**, in sede di collaudo, verificare che il fornitore/produttore sia regolarmente nominato Responsabile del trattamento dati all'atto della fornitura, provvedendo alla regolare formalizzazione del Ruolo mediante sottoscrizione del contratto e formale comunicazione all'UOC Privacy – Trasparenza e Integrità.
3) Per la esecuzione dei lavori agli immobili che richiedono accesso a locali/aree con possibile presenza di dipendenti, collaboratori, utenti, etc., identificando cosi un'attività di trattamento quale, il venire a conoscenza, (anche involontaria) dei dati degli interessati, o comunque la identificazione "*de visu*" degli stessi, compete all'**UOC Gestione Tecnico Patrimoniale e manutentiva**, trasmettere, tempestivamente, alla UOC Privacy – Trasparenza e Integrità, il provvedimento di aggiudicazione definitiva (delibera/determina) affinché quest'ultima possa procedere alla redazione del suddetto contratto per la formalizzazione del ruolo quale Responsabile ex art. 28 GDPR della ditta appaltatrice. Il suddetto provvedimento di aggiudicazione verrà inviato alla UOC Privacy – Trasparenza e Integrità mediante la procedura informatica Lapis-Web.
4) Per le convenzioni con soggetti esterni (associazioni di volontariato, …) che nello svolgimento delle loro attività trattano dati per conto del Titolare, compete alla **UOC Gestione degli Affari Generali** provvedere alla corretta classificazione di tali soggetti ed eventualmente, predisporre e redigere il relativo contratto di nomina quale Responsabile Esterno dei soggetti terzi, trasmettendone copia alla UOC Privacy – Trasparenza e Integrità, mediante la procedura informatica Lapis-Web, ovvero darne comunque ufficiale comunicazione dell'avvenuta sottoscrizione del contratto.
5) Per le convenzioni con soggetti esterni per le quali l'A.O. dei Colli, riveste il ruolo di Responsabile, atteso che svolge attività per conto di altri titolari (es. convenzioni di medicina di laboratorio) compete altresì alla **UOC Gestione degli Affari Generali**, proporre la relativa nomina, trasmettendone copia alla UOC Privacy – Trasparenza e Integrità, mediante la procedura informatica Lapis-Web, ovvero darne comunque ufficiale comunicazione dell'avvenuta sottoscrizione del contratto.
6) Per i contratti relativi a forniture di prodotti e servizi di cloud computing (SaaS, DaaS, PaaS, IaaS) e/o di servizi ICT in generale, in convenzione CONSIP/Altra centrale unica di committenza

nazionale o meno, che implicano trattamento dati, compete alla **UOC Ingegneria Clinica – HTA – SIA, anche nell'esercizio dei propri compiti in qualità di Direttore dell'esecuzione del contratto (DEC),** procedere in sede di aggiudicazione e/o esecuzione del collaudo, alla nomina di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 679/2016 del fornitore/produttore, trasmettendone copia alla UOC Privacy – Trasparenza e Integrità mediante la procedura informatica Lapis-Web, ovvero darne comunque ufficiale comunicazione dell'avvenuta sottoscrizione del contratto.

7) Per eventuali servizi integrativi, aggiuntivi e talvolta gratuiti in uso direttamente presso i reparti (es. sistemi di monitoraggio a distanza di pazienti cronici), non transitati, attraverso gli ordinari canali (convenzionamento e/o fornitura), compete ai **Direttori/Responsabili di UOC /UOSD**, utilizzatori di tali servizi, in qualità di Delegati interni al trattamento dati, proporre la nomina al Titolare, per il tramite dell'U.O.C Privacy – Trasparenza e Integrità.

Al fine di agevolare le procedure di Nomina quali Responsabili esterni del trattamento dati dei soggetti che trattano dati per conto del Titolare, i Direttori delle suddette U.O. riceveranno apposita Delega del Direttore Generale, quale Titolare del Trattamento, per la sottoscrizione dei relativi contratti.

La conservazione ed archiviazione degli eventuali contratti stipulati resta a carico delle strutture firmatarie, fermo restando l'inoltro di copia all'UOC Privacy – Trasparenza e Integrità, per gli adempimenti di competenza.

❖ DISPOSIZIONI FINALI

La presente procedura è stata adottata dal Titolare del trattamento, dal DPO, su proposta dell'U.O. C. Privacy – Trasparenza ed Integrità ed è in vigore il giorno successivo alla sua approvazione.

La sua pubblicizzazione, a cura U.O. C. Privacy – Trasparenza ed Integrità, avverrà nelle seguenti forme: attraverso la rete informatica interna e il sito aziendale

È fatto obbligo a chiunque spetti di osservarlo.

Il Responsabile della Protezione dei Dati (DPO) e la UOC Privacy –Trasparenza e Integrità sono a disposizione per eventuali dubbi, chiarimenti ed approfondimenti.

La presente procedura, nonché gli allegati che ne costituiscono parte integrante,sono suscettibili di eventuali modifiche, aggiornamenti ed integrazioni, nel caso le stesse si rendessero necessarie o opportune.

❖ AGGIORNAMENTI E NUOVI RILASCI

Aggiornamenti alla data del 01/01/2023.

Sono state apportate significative integrazioni al format relativo al "Contratto di nomina a Responsabile Esterno (Allegato n. 1)" che hanno riguardato:

- la indicazione dei dati di contatto del DPO del Responsabile Esterno, se nominato;
- la predisposizione di un ulteriore allegato al "Contratto di nomina a Responsabile Esterno (richiamato al par. 9.1)", riguardante la "Autorizzazione Generale del Titolare alla nomina di Sub-Responsabili del trattamento dei dati personali";
- la modifica all'Art. 12-Trasferimento dati verso Paesi Terzi, a seguito della "Decisione di esecuzione (UE) 2021/914 della Commissione Europea del 4 giugno 2021 relativa alle clausole contrattuali tipo (SCC) per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679".

Aggiornamenti alla data del 11/09/2023.

Sono state apportati aggiornamenti relativamente al capitolo "Stipula/revisione dei Contratti con i Responsabili del Trattamento Dati (ex art. 28 GDPR)" e al format relativo al "Contratto di nomina a Responsabile Esterno (Allegato n. 1)" consistenti in:

- la competenza per la nomina a Responsabile del trattamento dati (ex art. 28 GDPR), relativamente alla fornitura di prodotti e servizi ICT, è stata trasferita alla UOC Ingegneria Clinica – HTA – SIA (punto 6));
- il format del Contratto di nomina a Responsabile del trattamento dati (ex art. 28 GDPR) è stato sostituito con le clausole contrattuali tipo (SCC) emanate con Decisione di Esecuzione (UE) 2021/915 del 4 giugno 2021 dalla Commissione UE. Ciò in conformità dell'articolo 28, paragrafi 6 e 7, del regolamento (UE) 2016/679 ed in virtù dell'art. 1 della suddetta Decisione di Esecuzione che sancisce che tali clausole contrattuali tipo soddisfano i requisiti per i contratti tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafi 3 e 4.

CAPITOLO 4
ALLEGATI

CAP. 4

❖ DOCUMENTI ALLEGATI

Allegato n. 1	**Contratto di nomina a Responsabile Esterno**
Allegato n. 2	**VADEMECUM per R.E. ex art. 28 GDPR e Titolari Autonomi**

CONTRATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI in applicazione del REG. (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati, GDPR)

CONSIDERATO

- che l'Unione Europea ha introdotto il nuovo Regolamento Generale sulla Protezione dei Dati ("GDPR"), Regolamento (UE) 2016/679, applicato a partire dal 25 maggio 2018;
- che con d.lgs. n. 101 del 10/08/2018, denominato "Disposizioni per l'adeguamento della normativa nazionale al GDPR", il d.lgs. 196/2003 è stato adeguato alle nuove disposizioni europee;
- 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 l'oggetto e la durata del trattamento, la natura e lo scopo, il tipo di dati personali e le categorie di interessati trattati, gli obblighi e i diritti del Titolare;
- che è stata adottata la procedura aziendale di disciplina delle modalità operative interne per la ricognizione, identificazione e formale nomina dei "Responsabili esterni al trattamento dei dati" ai sensi del GDPR n. 679/2016;
- che nel medesimo provvedimento è stato stabilito che i trattamenti dei dati da parte di ciascun Responsabile esterno e le relative connesse responsabilità saranno compiutamente disciplinati da allegato apposito contratto, in conformità al paragrafo 3 dell'art 28 GDPR;
- 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 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" e che "i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento 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";
- che il Responsabile, nell'ambito delle attività/prestazioni professionali o 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;
- che il Responsabile non ha diritto ad alcun compenso specifico per l'esecuzione delle attività descritte in questo Accordo in quanto svolte nell'ambito dell'incarico in essere, per il quale è stata già definita l'intera valutazione economica del rapporto contrattuale;
- che il presente accordo annulla e sostituisce eventuali accordi precedentemente sottoscritti aventi lo stesso oggetto.

Sulla base degli assunti di cui sopra e, tenendo conto che con la DECISIONE DI ESECUZIONE (UE) 2021/915 del 4 giugno 2021 LA COMMISSIONE ha emanato le clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, e che tali clausole contrattuali tipo di seguito figuranti, soddisfano i requisiti per i contratti tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725, e che in conformità dell'articolo 28, paragrafo 6, del regolamento (UE) 2016/679 e dell'articolo 29, paragrafo 6, del regolamento (UE) 2018/1725, il titolare del trattamento e il responsabile del trattamento possono scegliere di utilizzare tali clausole, in tutto o in parte, in alternativa ad un contratto individuale, il Titolare del trattamento e il Responsabile del trattamento CONVENGONO di ADOTTARLE quale accordo tra le parti.

Clausole contrattuali tipo

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e/o dell'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

Clausola 2

Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679 o nel regolamento (UE) 2018/1725, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, rispettivamente.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 / dal regolamento (UE) 2018/1725, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

SEZIONE II

OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione 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 lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679/ il regolamento (UE) 2018/1725 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. **Limitazione delle finalità**

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 e/o dal regolamento (UE) 2018/1725. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di

revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento (Allegato IV) per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, 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 e/o del regolamento (UE) 2018/1725.

c) 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.

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

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento 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 del capo V del regolamento (UE) 2016/679 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.

Clausola 8

Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.In caso di esercizio dei predetti diritti, il responsabile darà tempestiva comunicazione scritta, e comunque non oltre il termine di 5 giorni dalla richiesta, al Titolare, allegando una copia della richiesta dell'Interessato, a mezzo **PEC/MAIL agli indirizzi ospedalideicolli@pec.it; rpd.ospedalideicolli@pec.it; rpd@ospedalideicolli.it.**

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo - entro 24 h - dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2) le probabili conseguenze della violazione dei dati personali;

3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo - entro 24 h - dopo esserne venuto a conoscenza. La notifica deve essere inviata a mezzo **PEC/MAIL agli indirizzi ospedalideicolli@pec.it; rpd.ospedalideicolli@pec.it; rpd@ospedalideicolli.it** e contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi;

d) ciascun responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni, secondo il disposto dell'art. 83 GDPR.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III

DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole 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 le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole 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 le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725;

3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto 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 delle presenti clausole.

ALLEGATO I

Elenco delle parti

Titolare/i del trattamento: [*Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]*

Nome: Azienda Ospedaliera dei Colli Monaldi-Cotugno-CTO

Indirizzo: Via Leonardo Bianchi, snc - 80131 Napoli

Nome e dati di contatto del referente: Direttore Generale (legale rappresentante protempore); ospedalideicolli@pec.it

Responsabile per la protezione dei dati (DPO): rpd.ospedalideicolli@pec.it; rpd@ospedalideicolli.it

Il Direttore Generale o, in delega, il Direttore U.O.C.:

Data di adesione:

Responsabile/i del trattamento [*Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]*

Nome:

Indirizzo:

Dati di contatto del referente:

Responsabile per la protezione dei dati (DPO):

Firma e data di adesione:

ALLEGATO II

Descrizione del trattamento (da compilare a cura del Responsabile)

Categorie di interessati i cui dati personali sono trattati

Categorie di dati personali trattati

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

Natura del trattamento

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento (inserire gli estremi della delibera/determina di affidamento del servizio)

Durata del trattamento

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati
(da compilare a cura del Responsabile)

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

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.

Di seguito descrivere le misure tecniche ed organizzative adottate relativamente a:

misure di pseudonimizzazione e cifratura dei dati personali;

misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

misure di identificazione e autorizzazione dell'utenti;

misure di protezione dei dati durante la trasmissione;

misure di protezione dei dati durante la conservazione;

misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati;

misure per garantire la registrazione degli eventi;

misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita;

misure di informatica interna e di gestione e governance della sicurezza informatica;

misure di certificazione/garanzia di processi e prodotti;

misure per garantire la minimizzazione dei dati;

misure per garantire la qualità dei dati;

misure per garantire la conservazione limitata dei dati;

misure per garantire la responsabilità;

misure per consentire la portabilità dei dati e garantire la cancellazione;

amministratore di sistema.

Nel caso in cui il responsabile eroghi i Servizi nel proprio Data Center, questo si impegna, **laddove necessario in base alla natura e tipologia dei servizi offerti,** a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "*Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento*", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.

In particolare il responsabile si impegna a:

- procedere alla designazione individuale degli Amministratori di Sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;
- 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;
- 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;
- 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.
- assicurarsi della qualità delle copie di back up e della loro conservazione in luogo sicuro e adatto, nonché della custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

Da compilare e sottoscrivere qualora il Responsabile ricorra ad altri Responsabili del trattamento dati

ALLEGATO IV

AUTORIZZAZIONE GENERALE DEL TITOLARE ALLA NOMINA DEI SUB-RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28, c. 2 del Regolamento U.E. 2016/679

TRA

L'Azienda A.O. dei Colli, con sede in Via L. Bianchi s.n.c. - 80131 Napoli, in persona del Direttore Generale, suo legale rappresentante *pro-tempore*

di seguito "*Titolare del trattamento*" o, per brevità, "*Titolare*"

E

Il/La _____,
con sede legale in _____, via _____,
n. _____, in persona del suo legale rappresentante _____,
nato a _____, il _____,
residente in _____, via _____,
n. _____, P.IVA/ Cod.Fisc. _____

di seguito "*Responsabile Esterno del trattamento*" o, per brevità, "*Responsabile*"

Premesso che:

- i termini e le espressioni inerenti alla normativa a tutela dei dati personali utilizzate nel presente atto hanno il significato ad essi attribuito dal Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("GDPR");
- tra Titolare e Responsabile è vigente un contratto stipulato in data _____, per effetto del provvedimento n. _____, per la prestazione di servizi erogati dal Responsabile in favore del Titolare avente ad oggetto _____ (di seguito indicato come "*Contratto*");
- tra le medesime società sopra individuate vige, altresì, apposito contratto contenente la disciplina degli obblighi in materia di protezione dei dati personali per le operazioni di trattamento oggetto del Contratto e necessarie per la sua esecuzione, in forza del quale il Titolare ha conferito al Responsabile - ai sensi e per gli effetti dell'art. 28 del GDPR - l'incarico di Responsabile del trattamento dei dati personali per conto del Titolare;
- il predetto contratto di nomina a Responsabile esterno per la disciplina degli obblighi in materia di protezione dei dati personali, di cui questa autorizzazione generale del Titolare costituisce parte integrante, prevede alla Clausola 7 par. 7.7 la facoltà – ai sensi dell'art. 28 par. 2 del GDPR - di avvalersi di altro soggetto esterno alla propria organizzazione, di seguito Sub Responsabile, cui affidare talune delle attività di trattamento;
- il soggetto individuato dal Responsabile per l'effettuazione di talune operazioni del trattamento deve, comunque, garantire ai sensi dell'art. 28 par.4 del GDPR gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento in materia di protezione dei dati personali,

fornendo, mediante un ulteriore contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che lo vincoli al Responsabile iniziale, le medesime garanzie di affidabilità e competenza tecnico-organizzativo richieste dal Titolare al Responsabile, anche sotto il profilo della sicurezza dei dati e dei trattamenti affidati;

- qualora un Sub Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub Responsabile;
- il Titolare, nella valutazione dei rischi determinati dall'affidamento/esternalizzazione verso il Responsabile dell'attività di trattamento, dovendo tener conto che le modalità di esecuzione di quella porzione di attività a questi, e agli eventuali Sub-Responsabili, affidata e che le misure che gli stessi si impegnano ad adottare, rispondano ai dettami previsti dal GDPR, avrà, comunque, facoltà di opporsi alla designazione di un eventuale Sub Responsabile effettuata dal Responsabile;
- il Responsabile iniziale, avendo il Titolare il potere di autorizzare, oppure negare, il ricorso ad un altro responsabile, all'atto della sottoscrizione della presente autorizzazione, fornisce sottoscritto in allegato, o in alternativa reperibile al seguente link: [ ], l'elenco aggiornato dei propri Sub Responsabili ed assume l'obbligo di informare il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Sub-Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche;
- ogni modifica al suddetto elenco si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 30 giorni. Qualora, invece, sollevi obiezioni, il Titolare fornirà al Responsabile le relative motivazioni il quale, a propria discrezione, potrà proporre un altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni oppure potrà adottare misure tese a superare le obiezioni del Titolare;
- Il Titolare autorizza espressamente che le operazioni di trattamento affidate al Responsabile, e da questi ad eventuali Sub Responsabili, possano essere svolte anche al di fuori dell'Unione Europea, purché il trasferimento di dati personali avvenga in presenza di una delle basi di legittimità previste dagli artt. 44 e ss. del GDPR. In particolare, laddove i dati personali vengano trasferiti verso un paese terzo in relazione al quale la Commissione Europea non abbia emanato una decisione di adeguatezza, il Responsabile si impegna a sottoscrivere e a far sottoscrivere ai Sub Responsabili designati, nonché, una volta sottoscritte a comunicarle al Titolare, le clausole contrattuali standard emanate dalla Commissione Europea o, in alternativa, si impegna a garantire e dimostrare che detti trasferimenti dei dati siano coperti dalla norme vincolanti d'impresa (BCR, Binding Corporate Rules) approvate dalla Commissione Europea.

Tutto ciò premesso e rilevato, l'**Azienda A.O. dei Colli**, come sopra identificata e nella qualità di Titolare del trattamento, con il presente atto

AUTORIZZA

Il/La [ ], nella qualità di proprio Responsabile del trattamento dati ai sensi dell'Art. 28 del GDPR, **ad incaricare**, **mediante un ulteriore contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri**, Sub-Responsabili per le operazioni di trattamento solo soggetti tra quelli inclusi nel suddetto elenco che assumono verso il Responsabile gli stessi obblighi in materia di protezione dei dati personali da questi assunti verso il Titolare.

Napoli, [ ]

IL TITOLARE DEL TRATTAMENTO

Il Direttore Generale o, in delega, il Direttore U.O.C.

[ ]

[ ]

PER ACCETTAZIONE

Il Responsabile del trattamento dei dati personali

[ ]

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi-Cotugno-CTO
Via L. Bianchi s.n.c. - 80131- Napoli
– C.F/P.I. 06798201213

All. 2

VADEMECUM

Responsabili Esterni

Il Rapporto tra Titolare (**A.O.R.N. Dei Colli**) e Responsabile (**Ditta Aggiudicatrice**) ai sensi dell'art.28 GDPR, si instaura, e quindi **dovrà essere inviato apposita nomina alla Ditta Aggiudicatrice, quando questa svolge, a titolo esemplificativo, i seguenti servizi**:

- Manutenzione dispositivi informatici
- Servizio di pulizie
- Servizio di portierato o vigilanza
- Servizio di trasporto
- Servizio di gestione delle telecamere per videosorveglianza
- Gestione delle licenze/ account e-mail
- Implementazione o gestione domino/sito internet
- Gestione dei corsi di formazione da remoto o in loco
- Gestione servizi in cloud
- Gestione fornitura elettronica
- Piattaforma per Distribuzione diretta del farmaco
- Contabilità analitica e generale dell'Azienda
- Piattaforma per Gestione telematica delle procedure di gara
- Servizio e gestione del CUP
- Custodia e Gestione cartelle cliniche (stoccaggio e rilascio copie)
- Servizi finalizzati alla custodia e alla riproduzione digitale copia documenti archivio
- App mobile che consente il Trattamento dati dei pazienti
- Servizio assistenza pacchetti applicativi informatici
- Attività che riguarda il volontariato
- Servizi per utilizzo, elaborazione, gestione e manutenzione del sistema RPM - Monitoraggio da remoto (es. fornitura di pacemaker/defibrillatori per monitoraggio a distanza cardiopatici)
- Attività finalizzate all' espletamento del servizio di telefonia fissa
- Attività finalizzate all' espletamento del servizio di sicurezza Applicativa
- Attività finalizzate all' espletamento dei Servizi di Connettività nell'ambito del Sistema Pubblico di Connettività

- Attività finalizzate alla fornitura e alla manutenzione delle Apparecchiature mediche (diagnostica per immagine, Tac)
- Servizi che consentono la Refertazione
- Servizi che riguardano attività per la Gestione del rischio clinico
- Eventuali altre attività e servizi che implicano trattamento dati

Titolari autonomi

In questo caso non dovrà essere inviata alcuna nomina.

A titolo esemplificativo, vi può essere questa tipologia di rapporto per:

- Attività assicurative
- Servizi bancari e di tesoreria
- Eventuali studi legali a cui si demandano controversie legali legate l'Azienda
- Studi notarili
- Attività di consulenza giuridico-economica