

**CONTRATTO DI NOMINA A
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**
in applicazione del Regolamento Generale sulla Protezione dei Dati
Art 28 - 2016/679 (GDPR)

TRA

L'Azienda Ospedaliera di Rilievo Nazionale Antonio Cardarelli, con sede legale in Napoli, via Antonio Cardarelli, P.IVA 06853240635, in persona del suo legale rappresentante, il Direttore Generale Dott. Antonio D'Amore

TITOLARE DEL TRATTAMENTO DEI DATI (anche semplicemente Titolare)

E

La _____ (con sede legale in _____

in persona del suo legale rappresentante _____ .nato a _____

il.....) residente in via

(P.IVA/Cod. Fisc.....) –

RESPONSABILE DEL TRATTAMENTO DEI DATI (anche semplicemente Responsabile)

PREMESSO

- che l'Unione Europea ha introdotto il nuovo Regolamento Generale sulla Protezione dei Dati ("GDPR"), Regolamento (UE) 2016/679, applicato a partire dal 25 2018;
- 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 con deliberazione del n° 924 . del 11/11/2019 con contestuali allegati, il cui contenuto si intende integralmente riportato e trascritto nel presente atto, 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. 2016/679,
- 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 comma 3 del precitato art 28 GDPR;
- che l'art. 4, c. 1, n. 8) del suddetto Regolamento 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, tra l'altro, 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 requisiti del presente regolamento e garantisca la tutela dei diritti

dell'interessato e che i trattamenti da parte del 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/la (....., .specificare i dati del responsabile), nell'ambito delle attività/prestazioni professionali o dei servizi affidati, ha i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno 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

Sulla base degli assunti di cui sopra, il Titolare e il Responsabile (anche semplicemente Parti) CONVENGONO quanto segue.

ART. 1 - OGGETTO DELL'ACCORDO

1.1. Le Parti, in virtù delle deliberazioni assunte dal Titolare e dei documenti ad esse allegati, con la sottoscrizione di questo Accordo, intendono disciplinare il trattamento dei dati personali da parte del Responsabile per conto del Titolare, specificando l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati e gli obblighi e i diritti delle Parti.

1.2 Il Titolare, nell'ambito delle attività/prestazioni professionali o dei servizi affidati al Responsabile, intende affidare a quest'ultimo, in conformità alle istruzioni da egli prescritte ed alle clausole del presente Accordo sul trattamento dei dati personali, le attività di trattamento di dati personali come di seguito dettagliate:

•[specificare l'oggetto dell'incarico o del servizio].

1.3 Il Titolare, pertanto, impegna il Responsabile, che con la sottoscrizione accetta, come "Responsabile" per il trattamento dei dati effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, funzioni e competenze come specificato dall'incarico in essere.

1.4 Il Responsabile ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

1.5 Il Responsabile fornirà attività/prestazioni professionali o servizi al Titolare in merito alla sua area di competenza, come specificato di seguito in questo Accordo. Nel contesto di tali attività/prestazioni professionali o servizi, il Titolare trasferirà al Responsabile alcuni dati personali che il Responsabile elaborerà e utilizzerà, per conto del Titolare, in conformità alle istruzioni scritte del Titolare e al presente Accordo.

ART. 2 – DEFINIZIONI

2.1 I termini utilizzati in questo Accordo hanno il seguente significato:

- "dati personali", "categorie speciali di dati personali", "processo/trattamento", "titolare", "responsabile", "interessato", "terzo" e "autorità di controllo" hanno lo stesso significato utilizzato nel GDPR;
- "misure tecniche e organizzative": misure volte a garantire un livello di sicurezza adeguato al rischio, volte a proteggere i dati personali dalla distruzione accidentale o illecita o dalla perdita accidentale, dall'alterazione, dalla divulgazione non autorizzata o dall'accesso ai dati personali trasmessi, archiviati o altrimenti trattati e contro tutte le altre forme illecite di trattamento;
- "violazione dei dati personali" o "data breach": violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o illegale di dati personali trasmessi, archiviati o altrimenti elaborati;
- "GDPR" - è l'acronimo del Regolamento Generale sulla Protezione dei Dati, Reg. (UE) 2016/679.

ART. 3 - AMBITO DEL TRATTAMENTO

3.1 I dettagli del trattamento dei dati sono:

a) Finalità: I dati relativi alle attività di trattamento di cui all'art. 1 sono trattati per le sole finalità relative all'incarico di attività/prestazioni professionali o servizi in essere ovvero:

[.....specificare l'oggetto dell'incarico o del servizio];

b) Natura del trattamento: le attività di trattamento di cui al precedente art. 1 e il conferimento dei dati interessati sono obbligatori in quanto la mancata fornitura non consentirebbe lo svolgimento delle suddette attività; tali dati sono nella generalità raccolti dal Titolare in occasione delle sue attività istituzionali e successivamente trattati dal Responsabile esterno per lo svolgimento delle proprie attività di servizio;

[.....inserire misure e procedure di sicurezza messe in essere per garantire il corretto lecito e trasparente trattamento dei dati ai sensi del GDPR 2016/679 (allegato 1)

c) Tipi di dati trattati: I dati personali trattati sono sia di tipo identificativo e non sensibile (es. nome e cognome, indirizzo di residenza, indirizzo email, codice fiscale, partita Iva, numero di telefono, etc.) che di tipo particolare (atti a rivelare lo stato di salute, l'adesione ad un sindacato, l'adesione ad un partito politico, l'origine razziale ed etnica nonché, convinzioni religiose o filosofiche; il trattamento dei suddetti dati personali e in special modo quello dei dati particolari, deve avvenire nel rispetto degli artt. 5 e 8 GDPR, anche alla luce del considerando n. 38 GDPR;

d) Soggetti interessati: Le attività di trattamento di cui al precedente art. 1 e i relativi dati trattati interessano soggetti nella sfera della titolarità del Titolare, quali pazienti minorenni e loro familiari, personale esercente la professione sanitaria, dirigenti e non dirigenti, dipendenti e collaboratori, clienti, fornitori, altri; va da sé che per i dati di cui sopra devono essere garantiti gli obblighi di trattamento nel rispetto dei principi di liceità, correttezza e trasparenza;

e) Durata del trattamento: La durata delle attività di trattamento di cui all'art. 1, e quindi il periodo di conservazione dei dati trattati, sarà limitato ad un arco di tempo non superiore al conseguimento delle finalità di cui alla lett. a) di questo articolo ed alla durata dell'incarico di Servizio in essere tra le parti, in ogni caso non oltre le tempistiche previste dalla Legge.

f) modalità di trattamento e di accesso ai dati: Nel caso fosse necessario intervenire da remoto sulle apparecchiature e/o software forniti, sarà indispensabile instaurare una connessione con la rete intranet dell'AO Cardarelli attraverso VPN o analoga tecnologia protetta.

A tal fine si precisa che l'autorizzazione all'accesso alla rete, sarà rilasciata al firmatario del presente contratto di Nomina di Responsabile del Trattamento che dovrà fornire a sua volta i nomi dei delegati al trattamento dei dati ai sensi del GDPR 2016/679 e del DLgs 101/18 art 2 quaterdieces.

E' fatto obbligo al Responsabile del Trattamento comunicare "ad horas" la cessazione del rapporto di lavoro del proprio dipendente precedentemente incaricato all'utilizzo della VPN o all'accesso da remoto e richiedere la sospensione dell'Account in caso di assegnazione personale al dipendente.

Viceversa, in caso di Account Aziendale, il Responsabile del trattamento deve provvedere alla richiesta di variazione della password al fine di poter continuare l'attività prevista.

ART. 4 - OBBLIGHI TITOLARE

4.1 Il Titolare del trattamento concorda e garantisce:

- **Conformità:** che è responsabile per la valutazione della legittimità del trattamento dei dati e nel garantire i diritti degli interessati coinvolti;
- **Sicurezza:** che le misure tecniche e organizzative adottate garantiscano un livello di sicurezza adeguato ai rischi presentati dal trattamento e dalla natura dei dati da proteggere, tenendo conto dello stato dell'arte e del costo della loro attuazione; di essere in grado di dimostrare che il trattamento è effettuato conformemente a quanto previsto dal Regolamento (UE) 2016/679;
- **Istruzioni:** che rilascerà istruzioni scritte riguardanti lo scopo e la procedura del trattamento dei dati, se del caso, amplificando, specificando e modificando le clausole di questo Accordo.

ART. 5 - OBBLIGHI RESPONSABILE

5.1 Il Responsabile del trattamento concorda e garantisce:

- ♣ **Competenza:** di possedere sufficienti conoscenze specialistiche nonché affidabilità e risorse per attuare misure tecniche e organizzative che soddisfino i requisiti del GDPR;
 - ♣ **Rispetto delle istruzioni del Titolare:** di trattare i dati personali solo per conto del Titolare e limitatamente alle attività di trattamento strettamente necessarie per l'espletamento delle funzioni, in conformità con le sue istruzioni documentate e il presente Accordo; se non è in grado di fornire tale conformità per qualsiasi motivo, informerà tempestivamente il Titolare che ha il diritto di sospendere l'elaborazione dei dati e/o risolvere il Contratto relativo alle attività/prestazioni professionali o dei servizi affidati e quindi il presente Accordo;
 - ♣ **Conformità alla legge:** che non ha motivo di ritenere che la legislazione applicabile impedisca di soddisfare le istruzioni ricevute dal Titolare e i suoi obblighi ai sensi del Contratto nell'ambito delle attività/prestazioni professionali o dei servizi affidati e del presente Accordo. Qualora ritenga che una modifica legislativa possa avere un sostanziale effetto negativo sulle predette garanzie e obblighi, ne darà prontamente notizia al Titolare che avrà il diritto di sospendere l'elaborazione dei dati e/o di risolvere il Contratto nell'ambito delle attività/prestazioni professionali o dei servizi affidati e quindi il presente Accordo;
 - ♣ **Misure tecniche e organizzative:** che, tenuto conto del rischio per i diritti e le libertà degli interessati, adotterà misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio che comprendano, tra l'altro, se del caso, le misure e le valutazioni di cui all'art. 32 del GDPR;
 - ♣ **Pronta notifica:** che informerà tempestivamente il Titolare del trattamento di:
 - qualsiasi richiesta legalmente vincolante per la divulgazione dei dati personali da parte di un'autorità giudiziaria, salvo laddove ciò sia proibito per rilevanti motivi di interesse pubblico;
 - qualsiasi violazione dei dati personali della quale verrà a conoscenza;
 - qualsiasi richiesta ricevuta direttamente dagli interessati;
 - qualsiasi istruzione scritta ricevuta dal Titolare che, secondo il parere del Responsabile, sia in violazione del GDPR e/o dei doveri di cui al presente Accordo.
 - ♣ **Dimostrazione di conformità:** di rendere disponibili al Titolare tutte le informazioni necessarie a dimostrare la conformità agli obblighi stabiliti nel presente Accordo e, su richiesta del Titolare, a presentare le proprie procedure di trattamento dei dati per la revisione delle stesse. Il Responsabile consentirà e contribuirà a tali verifiche, comprese le ispezioni, svolte dal Titolare o da un organismo di controllo da questi nominato;
- Cooperazione con Titolare per Autorità di Controllo: di collaborare con il Titolare per il rispetto di eventuali ordini emessi dall'Autorità di Controllo o dalle Autorità Giudiziarie in relazione al trattamento dei dati nonché di trattare tempestivamente e adeguatamente le richieste del Titolare in

relazione al trattamento dei dati e di attenersi alle linee guida dell'Autorità di Controllo in merito all'elaborazione dei dati.

ART. 6 - AMMINISTRATORI DI SISTEMA

Nel caso in cui il RESPONSABILE eroghi i Servizi nel proprio Data Center, questo si impegna 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.

Il RESPONSABILE si impegna, in particolare, a:

- a) procedere alla designazione individuale degli Amministratori di Sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;
- b) 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;
- c) 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;
- d) 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. e) 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.

7.1 Ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi di ordine generale.

7.2 Ai sensi dell'art. 5 GDPR, rubricato “Principi applicabili al trattamento dei dati personali”, per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate;
- i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare e rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

7.3 Ai sensi dell'art. 6 GDPR, rubricato "Liceità del trattamento", il Responsabile deve tenere conto che il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; i) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

7.4 Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Responsabile, che opera per conto del Titolare del trattamento, deve tenere conto, tra l'altro:

- a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
- c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'art. 10; delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- d) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

ART. 8 - COMPITI PARTICOLARI DEL RESPONSABILE

8.1 Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

1. individuare e nominare gli incaricati del trattamento per le banche dati che gli sono state affidate e fornirgli le istruzioni adeguate, vigilando sul rispetto delle stesse;
2. assegnare agli incaricati del trattamento, a seconda dei compiti attribuiti ad ognuno e laddove sia tecnicamente possibile, le credenziali di autenticazione che permettano di svolgere solo le operazioni di propria competenza nonché le dovute responsabilità per le aree ad accesso controllato, ove presenti;
3. ogni qualvolta si raccolgano direttamente dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
4. garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
5. adempiere gli obblighi di sicurezza e tutte le misure indicate dall'Art. 32 GDPR e assistere il Titolare del trattamento nel garantire il rispetto degli obblighi, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento. L'adesione da parte del Responsabile a un codice di condotta o a un meccanismo di certificazione può essere utilizzato come elemento per dimostrare le garanzie sufficienti.
6. cooperare, su richiesta, con il Responsabile della Protezione dei Dati Personali nell'esecuzione dei suoi compiti;
7. tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

8.mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente documento e consentire e contribuire alle attività di revisione, comprese le ispezioni, svolte dal Titolare del trattamento o da un altro soggetto da questi delegato/incaricato, informando immediatamente il Titolare del Trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;

9.fornire, secondo le modalità indicate dal Titolare, i dati e le informazioni necessari per consentire allo stesso di svolgere una tempestiva difesa relative al trattamento dei dati personali in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria;

10.redigere il registro dei trattamenti svolti, come da art. 30 GDPR;

11.collaborare, nel modo più ampio, con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal GDPR e segnalare eventuali problemi applicativi.

ART. 9 - ESECUZIONE DI SPECIFICHE ATTIVITA' DI TRATTAMENTO

9.1 Il Responsabile del trattamento non può affidare né ricorrere a un altro responsabile alcuna delle operazioni di trattamento dei dati senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. In caso di autorizzazione scritta generale, il Responsabile del trattamento informerà il Titolare del trattamento di eventuali modifiche relative all'aggiunta o alla sostituzione di altri Responsabili del trattamento, dando così al Titolare la possibilità di opporsi a tali modifiche, entro 30 giorni dalla notifica del cambiamento intervenuto.9.2 Nel caso il Responsabile del trattamento ricorra a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti in questo atto di nomina, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamenti soddisfi i requisiti del GDPR. 9.3 Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile nominato con il presente atto di nomina conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

ART. 10 - DIRITTI E RICHIESTE DEGLI INTERESSATI

10.1 Il Responsabile del trattamento comunicherà ogni informazione utile al fine di aiutare il Titolare a rispettare i diritti degli Interessati, ai sensi degli artt. 15-22 GDPR.10.2 Nella misura in cui ciò sia possibile, il Responsabile del trattamento assisterà il Titolare con adeguate misure tecniche e organizzative per l'adempimento dell'obbligo del Titolare di rispondere alle richieste di esercizio dei diritti degli Interessati.10.3 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

ART. 11 - COMUNICAZIONE DI DATI

Il Responsabile si asterrà dal comunicare dati personali oggetto del trattamento a terzi senza il preventivo consenso scritto del Titolare.

ART. 12 - TRASFERIMENTI VERSO PAESI TERZI

Il Responsabile del trattamento non può trasferire i dati personali provenienti dal Titolare al di fuori dello Spazio economico europeo (SEE) senza il previo consenso scritto e le istruzioni del Titolare, nel rispetto del presente Accordo e delle disposizioni atte a garantire la protezione dei dati personali di cui agli articoli del Capo V del GDPR, 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 vieti tale informazione per rilevanti motivi di interesse pubblico.

ART. 13 - RESPONSABILITÀ IN CASO DI VIOLAZIONE DEI DATI

13.1 In caso di violazione dei dati personali, il Responsabile del trattamento informa il Titolare del trattamento o il DPO dell'Azienda Cardarelli senza ingiustificato ritardo - entro 8 h dal momento in cui ne è venuto a conoscenza - della violazione, in modo che quest'ultimo possa provvedere a notificare la violazione al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dai motivi del ritardo. 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.

13.2 La comunicazione al TITOLARE dovrà essere inviata a mezzo PEC all'indirizzo direzione.generale@aocardarelli.it E-Mail del DPO dpo.privacy@aocardarelli.it _ entro e non oltre le 8h dal momento in cui il Responsabile è venuto a conoscenza della violazione e conterrà almeno le seguenti informazioni: 1) la natura della violazione dei dati personali, 2) la categoria degli interessati, 3) il contatto presso cui ottenere più informazioni, 4) i tempi trascorsi dall'incidente alla sua individuazione, ove determinabili, 5) i tempi di presa in carico, 6) gli interventi attuati o che si prevede di realizzazione e in che tempi. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

13.3 Inoltre, dato il dispositivo del primo comma dell'art. 82, secondo il quale chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal responsabile del trattamento, il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

13.4 Il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

13.5 Qualora più Responsabili del trattamento oppure entrambi il Titolare del trattamento e il Responsabile del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni Responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

13.6 Fatti salvo questi casi di responsabilità, se il Responsabile viola il GDPR, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

ART. 14 - CESSAZIONE E SUCCESSIVE OBBLIGAZIONI

14.1 Questo Accordo diventerà effettivo dalla firma delle Parti fino al termine del Contratto di "attività/prestazioni professionali o servizi" o al termine del trattamento dei dati per qualsivoglia motivo.

14.2 Alla cessazione del Contratto di "attività/prestazioni professionali o servizi" o del trattamento dei dati per qualsivoglia motivo il Responsabile del trattamento dovrà, a scelta del Titolare, restituire o cancellare i dati personali e le relative copie oggetto del trattamento dandone certificazione al Titolare, salvo che la legge preveda diversamente. In tal caso, per quanto riguarda i dati personali in questione, il Responsabile del trattamento ne garantirà la riservatezza e si impegnerà a non procedere più al loro trattamento.

ART. 15 - LEGGE APPLICABILE E FORO COMPETENTE

15.1 Il presente Accordo, salvo quanto diversamente ivi previsto, in linea con il GDPR, è regolato dalle leggi della giurisdizione del Titolare.

15.2 La sede esclusiva per tutte le controversie derivanti da o in connessione con questo Accordo è il luogo di stabilimento del Titolare, fatto salvo il diritto di quest'ultimo di presentare un'azione giudiziaria contro il Responsabile, di fronte a qualsiasi altro tribunale ritenuto competente.

ART. 16 - NORME FINALI

16.1 Salvo quanto previsto per il conferimento o la modifica delle istruzioni da parte del Titolare al Responsabile, il presente atto disciplina l'intero Accordo tra le Parti in relazione al suo oggetto. Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

16.2 Se una disposizione del presente Accordo è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni dello stesso rimangono inalterate. In questo caso, le Parti concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi delle Parti, come riportato nell'intera struttura del presente Accordo.

16.3 Salvo l'ipotesi di conferimento o variazioni delle istruzioni del Titolare previste dall'art 5, qualsiasi altra modifica delle clausole del presente Accordo può avvenire solo di comune accordo, comprovata dalla firma di entrambe le Parti dell'emendamento scritto. Le Parti possono anche aggiungere clausole su questioni relative all'attività di business, laddove necessario, purché non contraddicano le clausole di questo Accordo.

Napoli _____

per accettazione

**Il Responsabile Esterno del
Trattamento dei dati
AZIENDA_____**

**Il Titolare del Trattamento dati
Azienda AORN A. Cardarelli**

ALLEGATO 1

Misure di sicurezza adottate dal Responsabile

(istruzioni per la compilazione a cura del Responsabile: vedi note a piè di pagina)

SEZIONE A) – ELENCHI DI MISURE¹

	Agenzia di vigilanza notturna/diurna
	Antifurti interni
	Antifurti perimetrali
	Cancellate esterne con sbarramento
	Casseforti fisse
	Cassette di sicurezza mobili
	Pronto intervento con società esterna
	Estintori

	Generatori di corrente
	Illuminazione di emergenza
	Impianti antincendio fissi
	Inferriate alle finestre
	Porte blindate esterne
	Porte blindate interne
	Porte tagliafuoco
	Serrature armadi e/o cassettiere

	Serrature uffici
	Sistemi di condizionamento
	Strutture antisismiche
	Vetri antisfondamento
	Videosorveglianza

MISURE DI SICUREZZA INFORMATICHE

	Adozione di soluzioni informatiche per la gestione della compliance privacy
	Adozione di sistemi di conservazione a norma
	Antivirus
	Autenticazione informatica
	Autenticazione a più fattori
	Autorizzazione (privilegi di accesso)
	Backup
	Business Continuity Plan

	Cifratura dei dati "a riposo"
	Comunicazioni cifrate end-to-end
	Condivisione di documenti protetti con password tramite diverso canale
	Data Loss Prevention tools
	Disaster Recovery Plan
	Firewall hardware (fisico)
	Firewall software
	Log management
	Password management System

	Penetration test a cadenza periodica
	Pseudonimizzazione
	Remote wipe (cancellazione da remoto di dispositivi)
	Ridondanza geografica dei dati
	Separazione logica dei dati
	Security Operation Center (SOC)
	Network Operation Center (NOC)
	Virtual Private Network (VPN)

MISURE ORGANIZZATIVE

	Agenzia di vigilanza notturna/diurna
	Accesso controllato (privilegi di accesso fisico basati sul ruolo)
	Accordi di trattamento (DPA) con responsabili esterni (fornitori)
	Adesione a codici di condotta (art. 40 GDPR)
	Adesione a meccanismi di certificazione (art. 42 GDPR)
	Atti di autorizzazione e istruzioni di trattamento per gli operatori
	Atti di designazione (art. 2-quaterdecies Codice Privacy)
	Atti di autorizzazione e istruzioni di trattamento per gli operatori
	Sensibilizzazione, Formazione e Addestramento
	Nomine interne/esterne ad Amministratore di Sistema
	Audit interni di verifica
	Contratti di assicurazione contro i danni (es. cyber risks, data breach)
	Regolamenti o policy di utilizzo
	Separazione fisica di ambienti
	Servizio di vigilanza
	Procedure di gestione data breach
	Procedura di gestione dei riscontri all'interessato
	Canali dedicati per le comunicazioni (es. indirizzo e-mail specifico)
	Contratto con consulente privacy esterno
	Audit di terza parte
	Chiamata allo sportello senza indicazione nominativa
	Distanze di cortesia
	Designazione di un Data Protection Officer ("DPO")



REGIONE CAMPANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE
“A. CARDARELLI”
Via A. Cardarelli, 9 / 80131 - Napoli

² **Sezione A:** inserire una “**T**” se la misura è “Totalmente implementata”, inserire “**P**” se “Parzialmente implementata”, inserire “**N**” se “non implementata”.

³ **Sezione B:** da compilare ove possibile secondo le istruzioni seguenti:

- 1 fornire sintetiche informazioni sulle caratteristiche e sul contesto di utilizzo delle misure di sicurezza a protezione dei dati personali trattati per conto del Titolare indicate nella sezione A: **fisiche** (es. “la sala server è dotata di impianto di condizionamento che mantiene la temperatura tra i 15 e i 25°C; gli armadi collocati nell’Ufficio Acquisti sono dotati di serrature, le cui chiavi sono in possesso del solo responsabile”); **informatiche** (es. “siamo dotati di firewall di ultima generazione marca ... modello ...”, “vengono eseguiti backup settimanali su server di terza parte”); **organizzative** (es. “la formazione in materia di sicurezza informatica e privacy viene erogata annualmente su tutto il personale”);).
- 2 Inserire una sintetica spiegazione delle misure valorizzate con “**P**” (es. “esistono log degli accessi degli amministratori ma non di tutti gli utenti”; “esistono vetri antisfondamento unicamente nella sala server”) o “**N**” (es. “Il DPO non è stato designato in quanto non obbligatorio ai sensi e per gli effetti di cui all’art. 37 § 1.b Reg. UE 2016/679” oppure “La distanza di cortesia è inapplicabile ai servizi forniti al Titolare” oppure “In fase di valutazione” oppure “Pianificato e in via di implementazione”).