CONVENZIONE TRA LA ASL RIETI - UOC TUTELA DELLA SALUTE MATERNO-INFANTILE E L'OSPEDALE PEDIATRICO BAMBINO GESU' PER ATTIVITA' DI CONSULENZA IN AMBITO DI MEDICINA FETALE

TRA

l'AZIENDA SANITARIA LOCALE RIETI, C.F. e P. IVA 00821180577, con sede legale in Rieti, Via del Terminillo, 42 nella persona del Commissario Straordinario, Dott. Mauro Maccari, agli effetti del presente atto domiciliato in Rieti, Via del Terminillo n.42

E

L'**OSPEDALE PEDIATRICO BAMBINO GESU' – I.R.C.C.S.**, Istituto di Ricovero e Cura a Carattere Scientifico - Istituzione della Santa Sede, con sede legale in Roma, Piazza S. Onofrio 4, in una delle zone extraterritoriali riconosciute dal Trattato Lateranense del 1929 , Codice Fiscale 80403930581, nella persona del Dr Massimiliano Raponi, nella sua qualità di Direttore Sanitario dell'Ospedale e come tale munito di idonei poteri, parte denominata anche "OPBG"

PREMESSO

(le premesse sono parte integrante e sostanziale al presente atto)

- l'OPBG è una Istituzione della Santa Sede, che svolge attività assistenziale e caritatevole finalizzata alla cura dei pazienti in età pediatrica;
- l'OPBG, per effetto dell'art. 4 del D.Lgs. 502 del 30 dicembre 1992 e ss.mm.ii. e della Legge n.187 del 18 maggio 1995, di ratifica ed esecuzione dell'accordo del 15 febbraio 1995 tra il Governo Italiano e la Santa Sede, è incardinato nel Sistema Sanitario Italiano;
- l'OPBG, riconosciuto Istituto di Ricovero e Cura a Carattere Scientifico per la disciplina della pediatria, svolge attività di ricerca, diagnosi, ricovero e cura nelle diverse specialità per soggetti in età pediatrica ed evolutiva. L'Istituto promuove altresì il continuo progresso nelle metodiche diagnostiche e nelle terapie per il raggiungimento dei più elevati livelli scientifici e clinici;
- l'OPBG, in ragione dell'elevato livello di specializzazione, collabora con soggetti, enti ed istituzioni pubblici e privati, nazionali ed internazionali, per l'esecuzione di attività di assistenza, cura e ricerca, nell'ottica del perseguimento della finalità costitutiva dell'Ospedale;
- l'OPBG, in coerenza con la propria finalità costitutiva ed in ragione delle attività di assistenza, cura e ricerca in favore dei pazienti in età pediatrica, collabora alla realizzazione del bene materiale e spirituale della popolazione;
- che le parti hanno individuato, per la fase attuativa dell'accordo, rispettivamente:
  - Il Dott. Vincenzo Spina, Direttore della UOC Tutela della Salute Materno Infantile – della ASL di Rieti;
  - Il Dott. Giovanni Mosiello Responsabile pro-tempore della UOC Chirurgia della Continenza e Neurourologia dell'Ospedale Pediatrico Bambino Gesù.
- che, presso la UOC Tutela della Salute Materno-Infantile è attivo un Ambulatorio di Ecografia Ostetrica
- che detto Ambulatorio eroga esami ecografici di valutazione fetale nel primo, secondo e terzo trimestre di gravidanza
- che detto Ambulatorio è svolto da Professionisti esperti in Medicina Fetale, che operano secondo le procedure previste dalle *Linee Guida della Società Italiana di Ecografia in Ostetricia e Ginecologia* (SIEOG)

- che presso l'Ospedale Pediatrico Bambino Gesù è attivo un percorso per la presa in carico del feto dopo la nascita
- che presso la UOC Chirurgia della Continenza e Neurologia, dell'Ospedale Pediatrico Bambino Gesù, presta servizio Personale Medico Specialista con comprovata esperienza in Medicina Fetale e, in particolare, nella presa in carico prenatale delle patologie urologiche fetali
- che le patologie urologiche rappresentano problematiche di riscontro particolarmente frequente in epoca prenatale
- che il gold standard per la presa in carico delle patologie fetali suscettibili di trattamento prenatale o postnatale è rappresentato da un'attività di Consulenza Prenatale congiunta svolta da un'Equipe esperta in Medicina Fetale, composta da Ginecologi Ecografisti e Pediatri esperti
- che la collaborazione fra i due Centri ha l'obiettivo di assicurare il Percorso completo per il Neonato affetto da una patologia – specie se urologica - diagnosticata in epoca prenatale e suscettibile di trattamento prenatale o postnatale

SI CONVIENE E SI STIPULA QUANTO SEGUE

Art. 1
Oggetto

1.1 l'oggetto del presente Accordo è rappresentato dalla attivazione di una collaborazione tra la ASL Rieti - UOC Tutela Della Salute Materno-Infantile - e l'OPBG - finalizzata ad assicurare il Percorso completo per il Feto-Neonato affetto da patologia diagnosticata in epoca prenatale e suscettibile di trattamento prenatale o postnatale.

1.2 per la realizzazione di quanto sopra, in un concetto di rete assistenziale, le Parti condividono funzionalmente le *expertise* professionali ed il relativo Percorso assistenziale relativamente alle strutture interessate alla realizzazione della collaborazione in oggetto;

1.3 in particolare le Parti individuano, nel proprio ambito, le Strutture di riferimento assistenziali e di coordinamento delle attività che sono:
- per la ASL di Rieti, la UOC Tutela Della Salute Materno Infantile - Direttore Prof. Vincenzo Spina
- per l'OPBG, la UOC Chirurgia della Continenza e Neurologia, il cui Responsabile protempore è il Dr. Giovanni Mosiello

1.4 la collaborazione fra le Parti ha il compito di assicurare il Percorso completo per il feto-neonato e cioè:

- la presa in carico del feto e della Coppia Genitoriale afferenti alla Asl di Rieti, ove specificamente indicato, in fase prenatale attraverso una Consulenza congiunta svolta presso la ASL di Rieti da un'Equipe composta da Ginecologi ecografisti della ASL di Rieti, Urologo Pediatra afferente alla UOC Chirurgia della Continenza e Neurourologia dell'OPBG, Psicologo della ASL di Rieti
- la successiva presa in carico prenatale e postnatale, per gli approfondimenti e/o il trattamento ritenuti necessari, presso le articolazioni dell'OPBG idonee e specifiche per la determinata patologia del feto-neonato.

Art. 2
Obiettivi

2.1 **OBIETTIVO GENERALE**: favorire l'accesso alle tecniche diagnostiche e al trattamento delle patologie fetali, diagnosticate in epoca prenatale presso la ASL di Rieti

2.2 **OBIETTIVO SPECIFICO 1**: realizzare quindi un team-network operativo/organizzativo tra le Parti al fine di condividere le *expertise* professionali, strumentali e strutturali e creare un centro

polifunzionale che assicuri alla Coppia Genitoriale e al feto-neonato un percorso clinico –diagnostico-terapeutico, con particolare riferimento:

- requisiti di ammissione ed esclusione
- valutazione morfologica del feto
- valutazione funzionale, ove possibile, del feto
- valutazione della patologia fetale diagnosticata
- valutazione della opportunità-necessità di ulteriori approfondimenti diagnostici per meglio caratterizzare la patologia diagnosticata
- valutazione delle opzioni di trattamento – ove possibili – della patologia fetale diagnosticata
- valutazione – ove possibile – della prognosi della patologia fetale diagnosticata
- counselling ed acquisizione consensi informati
- Stesura dei consensi informati condivisi
- Attività scientifica

2.3 **OBIETTIVO SPECIFICO 2**: promuovere la conoscenza della possibilità di trattare diverse patologie fetali diagnosticate in epoca prenatale. Tale promozione avverrà attraverso convegni tematici, nonché campagne di informazione sul web e realizzazione di opuscoli informativi.

2.4 **OBIETTIVO SPECIFICO 3**: Formazione del Personale, con incontri di aggiornamento, riunioni collegiali con gli Operatori

Art. 3

Competenze

3.1***Competenze specifiche dei Centri aderenti al progetto***

ASL RIETI – UOC Tutela Della Salute Materno Infantile

1) Esame ecografico di primo livello
2) Contributo all'Equipe di Medicina Fetale con Personale Ecografista esperto in Medicina Fetale e Professionista Psicologo
3) Consulenza di Medicina Fetale svolta in collaborazione con Professionista della UOC Chirurgia della Continenza e Neurourologia dell'Ospedale Bambino Gesù
4) Coordinamento dei Medici Specialisti e Ricercatori afferenti al progetto ed operanti presso la struttura ospedaliera/ASL
5) Counselling psicologico

OPBG

1) Anamnesi e reclutamento pazienti
2) Contributo all'Equipe di Medicina Fetale con Professionista della UOC Chirurgia della Continenza e Neurorologia
3) Consulenza di Medicina Fetale, in forma congiunta a Professionisti Ecografisti della ASL di Rieti
4) Approfondimenti diagnostici effettuabili presso la ASL.
5) Effettuazione di Trattamenti postnatali e/o prenatali, se possibili e indicati a carico delle Strutture dedicate dell'Ospedale Pediatrico Bambino Gesù
6) Coordinamento dei medici specialisti afferenti al progetto ed operanti presso la ASL.
7) Counselling psicologico

3.2 ***Competenze comuni ai centri aderenti al progetto***

1. Condivisione requisiti di ammissione ed esclusione e stesura di protocolli e percorsi condivisi per l'accesso alle procedure diagnostiche e terapeutiche per le patologie fetali
2. counselling ed acquisizione consensi informati
3. follow up della Coppia Genitoriale-Feto-Neonato fino alla conclusione del caso clinico
4. Stesura dei consensi informati condivisi

3.3 *Strutture e operatori coinvolti - Referenti*

Per l'ASL di Rieti

- UOC Tutela Della Salute Materno Infantile – Direttore Prof. Vincenzo Spina - Referente Specialistico Prof. Vincenzo Spina
- Per la parte amministrativo/contabile - Referente Dott.ssa Albertina Battisti;

Per l'OPBG

1) per l'OPBG:

- Referenti specialistici: il Dr. Giovanni Mosiello, Responsabile protempore della U.O.C. Chirurgia della Continenza e Neurourologia, e il Dr Antonio Maria Zaccara, che garantiscono la corretta implementazione e il relativo monitoraggio della Convenzione per tutto quanto concerne la compiuta erogazione delle prestazioni e la connessa gestione operativa anche assicurando tutto quanto necessario per il rispetto dei correlati obblighi normativi, ivi inclusi quelli in materia di protezione dei dati personali. Il tutto garantendo anche le informazioni di natura meramente operativa, funzionali alla erogazione e/o acquisizione della prestazione, da fornire alla controparte.
- Referente amministrativo: il Dr Angelo Iunco, Responsabile protempore della Funzione Contabilità, Tesoreria e Bilancio, che garantisce la corretta implementazione e il relativo monitoraggio della Convenzione per tutto quanto concerne gli aspetti amministrativi, con particolare riferimento ai processi di fatturazione, ove applicabile. Il tutto garantendo anche le correlate informazioni da fornire alla controparte.
- Referente di coordinamento: il Dr Stefano Calamelli, Responsabile protempore del Servizio Attività LAPI, che garantisce la corretta implementazione e il relativo monitoraggio della Convenzione per gli ulteriori aspetti che non siano di natura strettamente specialistica ed operativa o amministrativa propria del Referente specialistico o del Referente amministrativo. Il tutto garantendo ogni connessa interlocuzione con la controparte anche afferente agli adempimenti normativi ivi inclusi quelli in materia di protezione dei dati personali.

Art. 4

Responsabilità

Ciascuna delle Parti assume i rischi per la responsabilità professionale correlata alle attività di competenza svolte dai propri medici specialisti in virtù del presente Accordo svolte presso la propria sede.

Resta chiaramente inteso che per le attività svolte dall'OPBG presso la ASL le stesse saranno ricomprese nella copertura della ASL così come previsto dalla vigente normativa in materia di responsabilità professionale (legge Gelli/Bianco).

Art. 5

Istruzioni Operative

Le parti ci impegnano a produrre ed a trasmettere alle Direzioni sanitarie aziendali della ASL Rieti e dell'Ospedale Pediatrico Bambino Gesù, le Istruzioni Operative entro 30 gg dalla stipula del presente accordo.

Art. 6

Durata della convenzione

Il presente Accordo ha la durata di anni n. 1 (uno), decorrente dalla data di ultima sottoscrizione e potrà rinnovarsi, previa valutazione dei risultati raggiunti, mediante atto scritto e firmato dai rispettivi Rappresentanti Legali ovvero dai soggetti muniti di idonei poteri di firma.

Ciascuna delle Parti potrà recedere dal presente Accordo - con preavviso di almeno 60 giorni - a proprio insindacabile giudizio, tramite comunicazione scritta.

Art. 7

Oneri economici

Dalla presente collaborazione non derivano per le Parti costi aggiuntivi rispetto a quelli che dovrà sostenere ciascuna per le attività svolte dal proprio personale impegnato nelle attività oggetto dell'Accordo.

Art. 8

Condotta etica e trasparenza

L'Ospedale Pediatrico Bambino Gesù ha adottato il Codice Etico disponibile sul sito web www.ospedalebambinogesu.it.

Ciascuna Parte si impegna ad agire nell'esecuzione del contratto nel rispetto della normativa vigente con correttezza e trasparenza evitando nel contesto del rapporto con l'Ospedale comportamenti, atti od omissioni che possano configurarsi quale mala gestio con finalità illecita e più in generale che si pongano in contrasto con i principi, i valori e le regole di condotta etica tali da poter generare per l'altra parte o il proprio personale responsabilità da atto illecito.

L'inosservanza degli obblighi e degli impegni sopra indicati costituisce inadempimento contrattuale con facoltà per la Parte non inadempiente di risolvere il contratto ai sensi e per gli effetti di cui all'art. 1456 del Codice Civile, fatte salve le azioni per il risarcimento del danno.

Art.9

Obblighi di riservatezza e trattamento dei dati personali

Le parti si impegnano a garantire la confidenzialità e la riservatezza dei dati trattati durante l'esecuzione della convenzione.

Le Parti dichiarano di rispettare le disposizioni in materia di protezione dei dati personali previste nel Regolamento Europeo n. 2016/679 (di seguito "RGPD") e nel D. Lgs. n. 196/2003, così come emendato dal D. Lgs. n. 101/2018, e di adempiere agli obblighi derivanti, adottando le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Nell'instaurazione ed esecuzione del rapporto disciplinato dal presente Accordo, i dati personali trattati si riferiscono a pazienti e a dipendenti, collaboratori e comunque qualsivoglia soggetto che opera in nome e per conto di ciascuna Parte.

Con riferimento al trattamento di dati personali di dipendenti, collaboratori e comunque di qualsivoglia soggetto che opera in nome e per conto di ciascuna Parte (nome, indirizzo e-mail aziendale ecc.), i dati saranno trattati dall'altra Parte unicamente per finalità strettamente correlate e funzionali alla instaurazione ed esecuzione del rapporto contrattuale disciplinato dal presente Accordo, nonché per adempiere ad eventuali obblighi di legge o di regolamento.

I dati saranno trattati nel rispetto dei principi di cui all'art. 5, par. 1 del RGPD, con le modalità meglio descritte nell'informativa ex art. 13 del RGPD che ciascuna Parte rende ai propri interessati e per il periodo di tempo strettamente necessario per il raggiungimento delle finalità sopra descritte.

Le Parti garantiscono che i soggetti interni coinvolti nel trattamento dei dati sono appositamente autorizzati, formati ed istruiti al fine di assicurare un'adeguata sicurezza e riservatezza dei dati personali trattati.

Con riferimento al trattamento di dati personali di pazienti effettuati nell'ambito del presente Accordo le Parti adotteranno i seguenti ruoli in base alle attività effettivamente svolte:

a. l'ASL in qualità di Titolare del Trattamento e l'Ospedale Pediatrico Bambino Gesù - IRCCS quale Responsabile del trattamento, giusto atto di nomina ai sensi dell'art.28 RGPD riportato in allegato (Allegato 1), per il servizio di consulenza reso presso l'ASL;

b. l'ASL e l'Ospedale Pediatrico Bambino Gesù – IRCCS, Titolari Autonomi del trattamento ciascuno per gli ambiti di propria competenza, ai sensi e per gli effetti dell'art. 4, comma par. 1, n. 7 del RGPD per quanto riguarda invece le attività di approfondimento e/o trattamento presso l'Ospedale.

Art. 10
Foro competente

Per qualsiasi controversia derivante dall'applicazione o dall'interpretazione del presente Accordo, le Parti preliminarmente si impegnano a comporre in via bonaria ogni eventuale conflitto e, solo nella impossibilità di raggiungere un accordo, le Parti espressamente convengono di accettare la giurisdizione esclusiva del Tribunale dello Stato della Città del Vaticano e successivi gradi, così derogandosi alla giurisdizione del Giudice Italiano.

Art.11
Registrazione

Il presente atto è soggetto a registrazione in caso d'uso. Le eventuali spese di bollo e registrazione sono a carico della Parte richiedente.

LETTO, CONFERMATO E SOTTOSCRITTO

Per l'ASL di Rieti	Per l'Ospedale Pediatrico Bambino Gesù
Il Commissario Straordinario Dott. Mauro Maccari	*Il Direttore Sanitario* *Dr Massimiliano Raponi*
_____	_____

Roma,_____

Allegato 1

AZIENDA SANITARIA LOCALE RIETI

Via del Terminillo, 42 – 02100 RIETI - Tel. 0746.2781 – PEC: asl.rieti@pec.it

www.asl.rieti.it C.F. e P.I. 00821180577

ATTO DI NOMINA

A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(ai sensi dell'art. 28 del Regolamento UE 2016/679)

TRA

ASL di Rieti con sede legale in Via del Terminillo 42, 02100 Rieti, in persona del legale rappresentante pro-tempore, quale Titolare del Trattamento, (di seguito, per brevità "Titolare" o "ASL" o "Azienda");

E

L'Ospedale Pediatrico "Bambino Gesù" - IRCCS, con sede legale in Roma, Piazza S. Onofrio n. 4, zona extraterritoriale in base del Trattato del Laterano, quale Responsabile Esterno del Trattamento (di seguito, per brevità, "Responsabile"),

Di seguito, congiuntamente, le "Parti".

PREMESSO CHE

(Le premesse formano parte integrante e sostanziale del presente Atto)

tra la ASL di Rieti e l'Ospedale Pediatrico "Bambino Gesù" è in atto una Convenzione finalizzata all'espletamento di attività consulenza in ambito di medicina fetale (di seguito, per brevità, "Convenzione");

per l'esecuzione delle attività previste nella Convenzione, il Responsabile tratterà dati personali di cui l'Azienda è Titolare;

l'ASL , in persona del legale rappresentante p.t., Titolare del trattamento dei dati personali, di "categorie particolari di dati personali" (già "dati sensibili" ai sensi del Codice Privacy) ed in particolare di "dati relativi alla salute" ai sensi degli artt. 4 e 24 del Regolamento UE 2016/679, ha pertanto individuato, l'Ospedale Pediatrico "Bambino Gesù", quale Responsabile Esterno del Trattamento medesimo sulla base delle evidenze documentali e delle dichiarazioni dallo stesso fornite al Titolare e della successiva verifica da parte di quest'ultimo, per quanto ragionevolmente possibile, della loro rispondenza al vero, circa le caratteristiche di esperienza, capacità e affidabilità che devono caratterizzare chi esercita tale funzione affinché il trattamento rispetti i requisiti della normativa vigente e garantisca la tutela degli interessati.

SI CONCORDA E SI STIPULA QUANTO SEGUE:

Art. 1
Definizioni

Ai fini del presente Atto di nomina valgono le seguenti definizioni:

Per "Legge Applicabile" o "Normativa Privacy", si intende il 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 (di seguito, per brevità, "GDPR") nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia ivi compresi il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e i provvedimenti dell'Autorità Garante per la Protezione dei dati personali applicabili alla fattispecie oggetto della Convenzione;

per "Dati Personali": si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire il Servizio di cui alla Convenzione stipulato con l'Azienda;

per "Categorie particolari di dati": si intendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

per "Dati relativi alla salute": si intendono i dati personali attinenti alla salute fisica e menatale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

per "Interessato": si intende la persona fisica cui si riferiscono i Dati Personali;

per "Servizio": si intende il servizio di consulenza specialistica reso dal Responsabile oggetto della Convenzione nonché il relativo trattamento dei dati personali, così come meglio descritto nel presente Atto di nomina;

per "Titolare": si intende, ai sensi dell'art. 4, par. 7 del GDPR, 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;

per "Responsabile del Trattamento": si intende, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

per "Ulteriore Responsabile": si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte del Servizio e che quindi tratta dati personali;

per "Persona autorizzata al trattamento" o "Incaricato": si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;

per "Amministratore di sistema" o "ADS": si intende la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;

per "Misure di Sicurezza": si intendono le misure di sicurezza di cui alla Normativa privacy;

per “Trattamento”: si intende, ai sensi dell'art. 4, par. 2 del GDPR, 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. 2
Nomina e oggetto

In attuazione dell'art. 28 del GDPR, l’Asl di Rieti, in qualità di Titolare del trattamento dei dati personali, di “categorie particolari di dati personali” (già “dati sensibili” ai sensi del Codice Privacy) ed in particolare di “dati relativi alla salute”, nomina l’Ospedale Pediatrico “Bambino Gesù” quale Responsabile dello stesso trattamento come previsto nella Convenzione, da intendersi quale parte integrante e sostanziale del presente atto, reso necessario per l'espletamento del Servizio.

Il Responsabile tratterà i Dati personali, così come specificati al precedente comma, di cui verrà in possesso/a conoscenza nello svolgimento del Servizio oggetto della summenzionata Convenzione solo in base a quanto ivi stabilito e a quanto previsto nel presente Atto.

Art. 3
Durata e finalità

Il presente Atto produce i suoi effetti a partire dalla data di sottoscrizione delle Parti e rimarrà in vigore fino alla cessazione delle attività svolte dal Responsabile a favore del Titolare, indipendentemente dalla causa di detta cessazione. Inoltre, fermo il diritto del Titolare di revocare, in qualsiasi momento e senza bisogno di motivazione, l’affidamento del Trattamento al Responsabile e/o la sua stessa nomina, il Trattamento, fatto salvo ogni eventuale obbligo di legge e/o contenzioso, avrà una durata non superiore a quella necessaria al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Art. 4
Modalità e istruzioni

Le modalità e le istruzioni per il Trattamento dei Dati Personali impartite dal Titolare al Responsabile sono specificatamente indicate e declinate nella summenzionata Convenzione e nella presente nomina.

In particolare, ai sensi e per gli effetti della vigente Normativa Privacy, il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, 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.

Il Titolare garantisce che tali dati siano stati acquisiti in conformità alla normativa sul trattamento dei dati personali e che i soggetti interessati abbiano ricevuto un’apposita informativa privacy.

In ragione della presente nomina, il Responsabile ha l’obbligo di attenersi, tra l’altro, alle seguenti istruzioni:

deve nominare formalmente tutte le persone autorizzate al trattamento dati (c.d. Incaricati), conferendo incarico scritto ai propri dipendenti e/o collaboratori che, sulla base delle relative competenze, effettuano i trattamenti di dati personali di competenza del Titolare e deve vigilare costantemente sull’operato degli stessi. Grava sul Responsabile la tenuta, la conservazione e l’archiviazione degli atti di nomina degli incaricati/persone autorizzate al trattamento dei dati. Tale documentazione è messa a disposizione del Titolare e/o dell’Autorità Garante per la protezione dei dati personali a semplice richiesta;

deve garantire che le persone autorizzate al trattamento dei dati personali siano costantemente formate e informate in materia di tutela dei dati personali e dei principi di conseguenza applicabili, e si siano impegnate alla riservatezza nello svolgimento dei propri compiti lavorativi o abbiano un adeguato obbligo legale di riservatezza;

deve assistere il Titolare nel garantire che il trattamento sia effettuato nei termini e nei modi stabiliti dalla normativa vigente in materia di protezione dei dati personali ivi compresi i provvedimenti e le linee guida emanate dalle Autorità di controllo, delle procedure adottate dal Titolare e nel rispetto delle presenti istruzioni;

deve assistere il Titolare nel garantire che il trattamento dei dati avvenga effettivamente in modo lecito e secondo correttezza nonché nel rispetto del principio di minimizzazione, assicurando che, fatti salvi eventuali obblighi di legge e/o contenzioso, i dati non siano conservati per un periodo superiore a quello necessario per gli scopi del trattamento medesimo;

tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, anche al fine di soddisfare possibili richieste per l'esercizio dei diritti dell'interessato, nonché per garantire il rispetto degli obblighi di cui agli artt. da 32 a 35 compresi del Regolamento, relativi alla sicurezza del trattamento, alla notifica ed alla comunicazione di una violazione dei dati personali e alla valutazione di impatto sulla protezione dei dati.

A questo fine, il Responsabile deve:

verificare costantemente l'efficacia delle misure di sicurezza adottate in conformità alla normativa vigente ed in linea con aggiornamenti e/o a eventuali perfezionamenti tecnici, che si rendano disponibili nel settore informatico;

relazionare, se richiesto, sulle misure di sicurezza adottate ed allertare senza ingiustificato ritardo il Titolare in caso di situazioni anomale o di emergenza che, a giudizio del Responsabile, possano risultare fonte di una violazione dei dati personali oggetto di trattamento;

accettare il diritto del Titolare alla verifica periodica dell'applicazione delle norme di sicurezza adottate (audit) ed assoggettarsi ad esso;

eseguire gli ordini del Garante o dell'Autorità Giudiziaria, salvo che il Titolare abbia tempestivamente comunicato la propria volontà di promuovere opposizione nelle forme di rito;

procedere, senza ingiustificato ritardo, alla segnalazione al Titolare di eventuali casi, anche solo presunti, di violazione di dati personali (da intendersi come tale la 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 personali trasmessi, conservati o comunque trattati), in linea con le norme e le procedure aziendali vigenti;

il Responsabile, per quanto di competenza, deve verificare periodicamente l'esattezza e l'aggiornamento dei dati che tratta per conto del Titolare, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;

il Responsabile, quando richiesto, deve mettere senza ingiustificato ritardo a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento consentendo e collaborando alle periodiche attività di revisione, comprese le ispezioni previamente concordate, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;

il Responsabile deve informare senza ingiustificato ritardo immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione da questi ricevuta violi il Regolamento o altre disposizioni, nazionali o dell'Unione,

relative alla protezione dei dati. Resta espressamente inteso che, laddove il Responsabile del trattamento abbia adempiuto integralmente ai compiti assegnatigli in forza del presente Atto e agli obblighi scaturenti dal RGPD, il Titolare risponderà comunque delle sanzioni e dei danni cagionati dal trattamento effettuato in violazione di legge, se ingiustificatamente rifiuta di effettuare i necessari interventi segnalati dal Responsabile e/o di adottare le misure dallo stesso suggerite;

il Responsabile deve tenere il Registro delle attività di trattamento svolte per conto del Titolare del trattamento ai sensi del comma 2 dell'art. 30 del Regolamento mettendolo senza ingiustificato ritardo a disposizione di quest'ultimo e/o del Garante a semplice richiesta;

il Responsabile assume con la sottoscrizione del presente Atto, specifico obbligo legale di riservatezza e confidenzialità nonché l'obbligo di concordare con il Titolare il corretto riscontro all'esercizio dei diritti degli interessati di cui agli artt. 15 e ss. del Regolamento;

il Responsabile deve garantire che nella propria organizzazione ogni accesso informatico ai dati trattati per conto del Titolare richieda l'assegnazione ad ogni incaricato di una specifica utenza individuale che abiliti al solo trattamento delle informazioni necessarie al singolo per lo svolgimento della propria attività lavorativa verificando almeno annualmente la permanenza in capo all'incaricato del relativo profilo di autorizzazione al trattamento;

nel processo di autenticazione, il Responsabile deve prevedere l'inserimento di un codice identificativo dell'incaricato associato a una parola chiave riservata (password) di adeguata complessità, comunicata all'incaricato in modalità riservata e modificata dallo stesso al primo utilizzo e successivamente con cadenza almeno trimestrale;

il Responsabile deve fornire istruzioni per non consentire che due o più incaricati al trattamento accedano ai sistemi, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente;

il Responsabile deve fare in modo che ogni incaricato, al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza, non lasci mai incustodito e accessibile lo strumento elettronico;

il Responsabile deve effettuare il salvataggio dei dati con finalità di backup e disaster recovery con cadenza almeno mensile e comunque prima di procedere al riutilizzo per altri scopi dei supporti di memorizzazione nel caso fosse necessario conservare le informazioni contenute negli stessi;

il Responsabile deve proteggere i dati personali trattati per conto del Titolare contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di adeguati strumenti elettronici da aggiornare con cadenza almeno settimanale;

il Responsabile deve aggiornare periodicamente e, comunque, almeno annualmente, i programmi per elaboratore con interventi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti;

il Responsabile deve adottare adeguate misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e, comunque, non superiori a sette giorni;

nell'ambito del trattamento dei documenti cartacei, il Responsabile deve:

individuare e configurare i profili di autorizzazione, per ciascun incaricato e/o per classi omogenee di incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento;

periodicamente verificare la sussistenza in capo agli incaricati delle condizioni per la conservazione per i profili di autorizzazione;

identificare gli eventuali soggetti ammessi ad accedere a categorie particolari di dati personali al di fuori dell'orario di lavoro;

identificare e comunicare agli incaricati gli archivi dove riporre i documenti contenenti i dati personali e/o categorie particolari di dati (armadi, stanze, casseforti, ecc.);

prevedere, ove possibile, la conservazione dei documenti contenenti dati personali di categorie particolari (i.e. sensibili e/o giudiziari) separata dai documenti contenenti dati personali comuni;

verificare la corretta esecuzione delle procedure di distruzione dei documenti, quando non più necessari o quando richiesto dall'interessato;

il Responsabile, al pari dei propri incaricati, deve inoltre:

trattare i dati personali e/o le categorie particolari degli stessi secondo il principio di limitazione della finalità, ovvero unicamente per lo scopo per cui sono stati raccolti;

non diffondere o comunicare i dati personali e/o le categorie particolari degli stessi a soggetti non autorizzati al trattamento;

non lasciare incustoditi documenti contenenti i dati personali e/o le categorie particolari degli stessi durante e dopo l'orario di lavoro;

non lasciare in luoghi accessibili al pubblico i documenti contenenti i dati personali e/o le categorie particolari degli stessi;

riporre i documenti negli archivi quando non più operativamente necessari;

limitare allo stretto necessario l'effettuazione di copie dei suddetti documenti.

Laddove rilevante ai fini dei servizi e delle attività di cui alla Convenzione, in ottemperanza a quanto previsto dal Provvedimento del Garante Privacy del 27 novembre 2008, e sue successive modificazioni, riguardante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" e s.m.i., il Responsabile si impegna, altresì, ad adempiere a tutti gli obblighi prescritti dai predetti Provvedimenti, tra cui, in particolare:

individuare e designare quale "Amministratore di Sistema" la/e persona/e cui sono attributi compiti e/o funzioni di Amministratore di Sistema in riferimento ai sistemi impegnati per la fornitura dei servizi oggetto della Convenzione, previa valutazione dei requisiti di esperienza, capacità ed affidabilità di tali persone e con l'elencazione analitica nella designazione individuale degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

mantenere un documento interno aggiornato, contenente gli estremi identificativi delle persone preposte quali Amministratori di Sistema, con l'elenco delle funzioni ad esse attributi, e renderlo disponibile in caso di accertamenti del Garante e, ove necessario, di verifica da parte del Titolare, su richiesta di quest'ultima;

adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi ed archivi elettronici da parte degli Amministratori di Sistema designati, assicurando che le registrazioni abbiano le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità prescritte dal citato Provvedimento e siano conservate per almeno 6 mesi;

adottare per tutti i sistemi Sw di base ed Hw che prevedano un'utenza di super user, che non possa essere identificata fisicamente con un Amministratore di Sistema, la creazione di un registro ove siano riportate i dati anagrafici dell'utente incaricato di svolgere tale attività; Qualora gli utenti incaricati per accedere al medesimo Sw di base ed Hw fossero più di uno, in tale registro dovrà essere previsto il controllo quotidiano delle presenze in servizio di tali incaricati al fine di poter ricondurre le attività svolte sui sistemi ai medesimi amministratori;

procedere, annualmente, alla verifica dell'operato dei suddetti Amministratori di Sistemi, in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati connessi ai servizi forniti alla nostra Azienda;

produrre ed aggiornare annualmente, se richiesto, un documento attestante i servizi svolti che contenga anche la copia degli attestati della formazione del personale incaricato allo svolgimento delle attività e spieghi esaustivamente tuti processi svolti al fine del mantenimento della sicurezza dei dati.

dopo esserne venuto a conoscenza, avvisare senza ingiustificato ritardo il Titolare, scrivendo all'indirizzo "dpo@asl.rieti.it", di ogni violazione dei dati personali trattati per conto di quest'ultimo. Il Responsabile fornirà al Titolare ogni collaborazione anche ai fini del rispetto di quanto previsto dagli artt. 33 e 34 del GDPR;

avvisare senza ingiustificato ritardo, scrivendo all'indirizzo "dpo@asl.rieti.it", il Titolare di ogni richiesta, ordine od attività di controllo di cui venga fatto oggetto da parte del Garante, dell'Autorità Giudiziaria o di altra Pubblica Autorità sui dati personali trattati dall'Azienda Sanitaria in qualità di Titolare, nei limiti in cui ne sia consentita la comunicazione. Il Responsabile, che in tal senso fin d'ora si impegna nei limiti di quanto di sua competenza, assisterà il Titolare del trattamento nel garantire il rispetto degli obblighi derivanti da ordini del Garante, dell'Autorità Giudiziaria o di altra Pubblica Autorità;

informare, altresì, tempestivamente, scrivendo all'indirizzo "dpo@asl.rieti.it", e comunque entro sette (7) giorni lavorativi, il Titolare delle istanze formulate nei suoi confronti, ai sensi degli artt. 15 e ss. del Regolamento, da parte degli interessati dalle operazioni di trattamento connesse all'esecuzione del Servizio ed

in riferimento ai dati personali trattati per conto del Titolare al quale fornirà ogni necessario supporto per garantire il corretto riscontro. Il Responsabile, tenendo conto della natura del trattamento, è tenuto ad assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

Fatto salvo quanto precede, il Titolare prende atto delle misure di sicurezza di cui all'Allegato 2 quali attualmente applicate dal Responsabile.

Art. 5
Obblighi e doveri del Responsabile del trattamento

Il Responsabile, al momento della sottoscrizione del presente Atto, dichiara e garantisce di possedere una struttura ed una organizzazione adeguata per l'esecuzione del Servizio e si impegna ad adeguarla ovvero a mantenerla adeguata alla delicatezza della nomina, garantendo il pieno rispetto (per sé e per i propri dipendenti e collaboratori interni ed esterni) delle istruzioni sul trattamento dei dati personali specificatamente indicate e declinate nella Convenzione, nella presente nomina, oltre che della Normativa Privacy.

Art.6
Tipologie di dati, finalità e categorie di interessati

Il Responsabile svolge per conto del Titolare le attività di Trattamento dei Dati Personali relativamente alle tipologie, alle finalità ed alle categorie di soggetti esplicitate nel Servizio di cui alla Convenzione, parte integrante e sostanziale del presente Atto di nomina.

Art.7
Nomina di ulteriori responsabili

In esecuzione e nell'ambito del Servizio, il Responsabile, ai sensi dell'art. 28 comma 2 del GDPR, è autorizzato, salva diversa comunicazione scritta del Titolare, a ricorrere alla nomina di Ulteriori Responsabili ad esso subordinati, previo esperimento delle necessarie procedure di selezione dei fornitori applicabili di volta in volta.

Il Responsabile è tenuto, in sede di individuazione degli eventuali Ulteriori Responsabili e/o della loro sostituzione, ad informare preventivamente il Titolare, al fine di consentire a quest'ultimo, in attuazione dell'art. 28 comma 2 summenzionato, di poter manifestare eventuale formale opposizione alla nomina entro e non oltre il congruo termine di 20 (venti) giorni dalla ricezione della comunicazione. Decorso detto termine, il Responsabile potrà procedere all'effettuazione delle nomine, normativamente previste, nei confronti degli Ulteriori Responsabili individuati.

La nomina di un Ulteriore Responsabile da parte del Responsabile sarà possibile a condizione che sull'Ulteriore Responsabile siano 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 nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalla Normativa Privacy.

Qualora l'Ulteriore Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'Ulteriore Responsabile.

Il Responsabile, infine, si obbliga a comunicare al Titolare, con cadenza annuale, eventuali modifiche ed aggiornamenti dei trattamenti di competenza dei propri Ulteriori Responsabili.

Art.8
Vigilanza, sanzioni e responsabilità

Ai sensi e per gli effetti dell'art. 28, comma 3 del GDPR, al fine di vigilare sulla puntuale osservanza della Legge Applicabile e delle istruzioni impartite al Responsabile, il Titolare, anche tramite il proprio Responsabile della Protezione Dati e/o altro soggetto allo scopo individuato, potrà effettuare periodiche azioni di verifica preventivamente concordate con il Responsabile. Tali verifiche, che potranno anche comportare l'accesso a locali o macchine e programmi del Responsabile Esterno, potranno aver luogo a seguito di

comunicazione da parte del Titolare, da inviare con un preavviso di almeno cinque giorni lavorativi. Nell'ambito di tali verifiche, il Responsabile fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste del Titolare, in relazione ai dati e ai trattamenti rispetto ai quali ha valore il presente atto di nomina.

Le Parti del presente Atto sono soggette, da parte dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Il Responsabile assume piena responsabilità diretta verso gli Interessati per il danno causato dal trattamento 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.

Art. 9
Disposizioni Finali

Il presente Atto di nomina, in uno con la Convenzione, deve intendersi quale contratto formale che lega il Responsabile al Titolare del trattamento e che contiene espressamente le Istruzioni documentate del Titolare, le modalità di gestione dei dati, la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento, così come le responsabilità in ambito privacy.

Con la sottoscrizione, il Responsabile accetta la nomina e si dichiara disponibile e competente alla piena attuazione di quanto nella stessa previsto.

La presente nomina ha carattere gratuito e ha durata pari alla durata della Convenzione a cui accede o, comunque, dell'atto giuridicamente vincolante che ne forma presupposto indefettibile e, fermo quanto indicato al precedente art. 3, si intenderà, pertanto, revocata al venir meno dello stesso, indipendentemente dalla causa, ovvero, in qualsiasi momento, per insindacabile decisione del Titolare.

LETTO CONFERMATO E SOTTOSCRITTO

Il Responsabile Esterno
Ospedale Pediatrico "Bambino Gesù"
Il Direttore Sanitario
Dr Massimiliano Raponi

Il Titolare del trattamento
ASL Rieti

FIRMATO DIGITALMENTE

FIRMATO DIGITALMENTE

Allegato 2

(Misure organizzative e tecniche adottate dal Responsabile)

Indice

***

1. Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

2. Autenticazione

2.1 Credenziali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla creazione di una *password* alfanumerica di almeno 8 caratteri in lunghezza, contenente maiuscole/minuscole e caratteri speciali. In alternativa, il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire il possesso di un *token* o, per trattamenti di particolare rilevanza in termini sia legali che di criticità per il core business aziendale del Titolare, la verifica di caratteristiche biometriche univoche e univocamente digitalizzabili come ad esempio l'impronta digitale. Il Responsabile e gli eventuali Sub-Responsabili si impegnano, eventualmente, su espressa richiesta del Titolare, a procedere alla combinazione di due o più fattori di autenticazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad applicare i criteri summenzionati su tutti i sistemi e applicazioni aziendali.

2.2 Segnalazione inattività

Il Responsabile e gli eventuali Sub-Responsabili si impegnano affinché tutte le credenziali, eccetto quelle utilizzate per soli scopi di gestione tecnica, quali utenze macchina o credenziali di root, vengano segnalate come inattive dopo sei mesi.

2.3 *Non disclosure*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare opportune procedure per accedere ai dati in caso di assenza prolungata dell'incaricato che li detiene. Tali procedure non dovrebbero in alcun caso prevedere la *disclosure* della *password* dell'incaricato.

3. Salvaguardia dati e dispositivi

3.1 Protezione delle credenziali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una *policy* contenente delle chiare istruzioni circa le cautele da adottare per assicurare la segretezza delle credenziali e la diligente custodia dei dispositivi assegnati.

3.2 Protezione da danni e furti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una *policy* contenente delle chiare istruzioni circa le cautele da adottare per assicurare la salvaguardia dei dispositivi assegnati.

3.3 Protezione delle sessioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad implementare un sistema di *lock screen/screensaver* con reinserimento delle credenziali ogni qualvolta non vi è fisicamente un incaricato presente a presidiare/utilizzare la postazione di lavoro. Tale *lock screen* dovrebbe essere impostato affinché si attivi in automatico dopo meno di 5 minuti di inattività.

4. Autorizzazione

4.1 Esistenza profili autorizzativi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un sistema centralizzato per la gestione di autenticazione e autorizzazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad un censimento dei permessi effettivamente da attribuire, prima di procedere con la loro assegnazione.

4.2 Minimizzazione dei permessi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere in via residuale, non assegnando più permessi del dovuto e tenendo a mente i principi del *least privilege* e del *need to know* ossia consentendo la visualizzazione dei soli dati necessari a svolgere la funzione lavorativa, con attribuzione dei permessi minimi su sistemi e applicativi.

5. Difesa

5.1 Aggiornamenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare e gestire in maniera centralizzata e/o automatizzata gli aggiornamenti, o ad adottare idonei mezzi organizzativi in maniera tale da rendere le macchine e le applicazioni costantemente aggiornate tenendo in particolare considerazione gli aggiornamenti di sicurezza.

5.2 Isolamento sistemi non più supportati

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a segregare le macchine che per ragioni di operatività vengono ancora utilizzate nonostante non siano più supportate da aggiornamenti.

5.3 *Data protection by design*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare o adottare delle linee guida di *data protection by design*, assicurandosi che i sistemi aziendali sviluppati internamente siano coerenti con esse.

5.4 Programmi di protezione allo stato dell'arte

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e mantenere aggiornati i *software* di protezione quali antivirus, la cui gestione dovrebbe avvenire in maniera preferibilmente centralizzata, *firewall*, contenente preferibilmente moduli IDS e IPS, *antispam*.

6. Disponibilità dati

6.1 *Backup*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a implementare un sistema di *backup*, formalizzando un piano di *backup*, documentando le tecnologie in atto all'interno di una *policy* contenente altresì una procedura per eseguire correttamente tale attività.

6.2 Piani di ripristino

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad effettuare test di ripristino, verbalizzare i test effettuati e le procedure di ripristino, documentando, inoltre, i tempi necessari per eseguirle.

7. Protezione dati

7.1 Cifratura e confinamento

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare tecniche di cifratura a tutti i livelli: *full disk encryption* sulle unità di massa, *transparent data encryption* sui *database*, *file-level encryption* per file contenenti credenziali, tramite l'utilizzo di standard crittografici non deprecati.

7.2 Pseudonimizzazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla pseudonimizzazione dei dati personali eventualmente presenti all'interno dei *database*.

7.3 Cifratura in transito

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare le tecnologie di cifratura in transito.

8. Dispositivi rimovibili

8.1 Dispositivi rimovibili

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a regolamentare l'utilizzo dei supporti rimovibili e la loro protezione.

8.2 Sanitizzazione dei dispositivi rimovibili

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare opportune procedure per la distruzione, cifratura e/o formattazione dei dispositivi rimovibili e dei dispositivi aziendali in uso.

9. Ruoli di sicurezza

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a definire la funzione aziendale che sia responsabile per la *cybersecurity*, ossia chi possa ricoprirla in azienda con le relative responsabilità. Ciò può comportare di designare un CISO (*Chief Information Security Officer*) o, più generalmente, un CSO (*Chief Security Officer*) o, generalmente, una figura che abbia l'autorità, in azienda, di perimetrare, sotto il piano della sicurezza, informatica e delle informazioni, i processi dell'organizzazione. Tale figura dovrebbe essere reperibile al fine di riscontrare eventuali incidenti di sicurezza e dovrebbe essere nota a tutti i dipendenti.

10. Terze parti

10.1 Contratti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere tutti i contratti rilevanti con gli outsourcer e con i fornitori in maniera tale che includano anche i requisiti di sicurezza pertinenti al servizio o prodotto fornito.

10.2 Audit di secondo livello

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a verificare periodicamente la coerenza con i requisiti di sicurezza contrattualizzati tramite audit di secondo livello opportunamente contrattualizzati e calendarizzati.

11. Asset Management

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rimuovere *asset* e credenziali degli impiegati non più in forze all'interno dell'infrastruttura del Responsabile e Sub-Responsabile, o che abbiano cambiato mansione e asset necessari per svolgere la mansione.

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare una verifica periodica dell'effettiva rimozione di asset e credenziali.

12. Sicurezza fisica del Centro Elaborazione Dati (“CED”)

Questa sezione tratta la sicurezza fisica del Centro Elaborazione Dati (CED), dove i dati saranno ospitati e/o elaborati. Si applica sia nel caso di CED direttamente posseduti o controllati dal Responsabile ed eventuali Sub-Responsabili, sia nel caso di risorse fornite da un Fornitore di Servizi (ad esempio un provider di servizi in Cloud); in questo secondo caso, il Responsabile ed i Sub-Responsabili devono assicurarsi che il Fornitore di Servizi garantisca i livelli di sicurezza indicati.

12.1 Misure di sicurezza fisica

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere e implementare procedure formali di accesso per consentire l'accesso fisico al CED. I server e le macchine sulle quali sono conservati i dati del Titolare, all’interno del CED, sono ospitati in strutture che richiedono l'accesso con chiave dotata di scheda elettronica, con allarmi collegati ad eventuali SOC o centri di monitoraggio della sicurezza fisica. Le richieste di accesso alle chiavi dotate di schede elettroniche devono essere sottoposte ad un processo formalizzato di approvazione.

12.2 Visitatori

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad autenticare i visitatori prima dell’accesso al CED. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad accompagnare all’interno della struttura del CED i visitatori e di predisporre un registro di accesso degli stessi. Al fine accedere all’infrastruttura del CED, i visitatori dovranno (i) ottenere in anticipo l'approvazione da parte dei responsabili del CED per le aree interne che desiderano visitare; (ii) accedere tramite identificazione in loco.

12.3 Condizioni del CED

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare costantemente le condizioni del CED, considerando le variabili relative, tra le altre, a temperatura, condizione dell’impianto di raffreddamento, polvere, umidità e a verificare periodicamente il funzionamento dei sensori.

13. Controllo degli accessi

13.1 Credenziali individuali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a creare credenziali individuali per ciascun incaricato e istruire gli stessi incaricati circa la necessità di non condividere le credenziali.

13.2 Presenza di profili autorizzativi

Il Responsabile e gli eventuali Sub-Responsabili si impegnano, nei limiti di quanto consentito dai sistemi, a creare dei profili autorizzativi ai quali assegnare le utenze create.

13.3 Network access control

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a valutare la possibile introduzione di una soluzione per il NAC (*Network Access Control*) allo scopo di autenticare le macchine sulla rete.

13.4 Separazione VLAN

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione la possibilità di segmentare la rete in VLAN separate.

13.5 Sessioni concorrenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di sessioni concorrenti sui sistemi per lo stesso utente.

13.6 *Rate limiting*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di tentativi falliti di login prima del blocco dell’account su tutti i sistemi e applicativi aziendali.

14. Integrità dei sistemi

14.1 *SQL Injection*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad attenzionare e implementare processi di sanitizzazione degli input al fine di scongiurare attacchi noti quali SQL Injection.

14.2 Gestione password e chiavi di cifratura

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare soluzioni per la gestione di password e chiavi di cifratura.

14.3 Assenza di possibile disattivazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a non consentire agli incaricati, non preposti a funzioni di sicurezza, di poter disattivare le misure di protezione sulle loro macchine.

15. Vulnerability assessment e penetration testing

15.1 Periodicità

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a condurre sessioni di *vulnerability assessment* e *penetration testing* sui sistemi aziendali con periodicità almeno annuale.

15.2 Automatizzazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad impiegare dei tool per il *Vulnerability Assessment* automatizzato, che tuttavia non deve sostituire quello tradizionale.

16. Gestione degli incidenti e delle violazioni

16.1 Procedure di *incident handling*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a introdurre prassi, protocolli e procedure relative all'*incident handling* e gestire tutti gli eventi di sicurezza e/o gli incidenti di sicurezza tramite una procedura formalizzata con dei ruoli prestabiliti.

16.2 Formazione del personale

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere edotto il personale relativamente alle procedure di *incident handling*.

16.3 *Alert*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione, se ritenuto funzionale e adeguato al rischio, ad adottare un SIEM, o soluzioni alternative che raggiungano lo scopo di segnalare anomalie e/o attacchi in corso.

16.4 Registro degli incidenti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a stilare e mantenere un registro degli incidenti, che contenga almeno le informazioni in merito a scoperta, analisi, contenimento, mitigazione e recupero dai vari incidenti di sicurezza.

16.5 Comunicazione al titolare

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a comunicare tempestivamente, nell'arco di 24 ore dalla scoperta, gli incidenti di sicurezza occorsi sulle loro infrastrutture al Titolare.

17. Business continuity e Disaster Recovery

17.1 *Business continuity*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire la continuità operativa per tutti i servizi offerti al Titolare, tramite, se del caso, la formalizzazione di un *Business Continuity Plan*.

17.2 *Disaster recovery*

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere possibile il ripristinare tutti i dati del Titolare in seguito a disastri, tramite, se del caso, la formalizzazione di una strategia per il *Disaster Recovery*, includendo *policy* dettagliate per la conservazione sicura delle copie di *backup* e loro ripristino.

17.3 Cifratura e custodia

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prevedere la cifratura del *backup* e di prevedere procedure sicure per la loro custodia.

18. Formazione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare training periodici di *security awareness* per tutto il personale d'ufficio, al fine di ridurre l'eventualità di intrusioni, riuscita di *phishing* o infezione da malware.

19. Registrazione delle operazioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un *software* di *operational intelligence* che produca log inalterabili, completi e passibili di verifica d'integrità che operi sui sistemi sui quali sono trattati i dati personali riferibili al Titolare.

20. Sviluppo software e gestione ambienti

20.1 Linee guida sviluppo

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e adottare linee guida di scrittura del codice sicuro.

20.2 Separazione ambienti

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a separare gli ambienti di *test*, sviluppo e produzione.

20.3 Formalizzazione dei processi di produzione

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare le procedure necessarie al passaggio dall'ambiente di *test* all'ambiente di produzione.

20.4 Testing

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a testare *software* e sistemi previo inserimento in produzione.

20.5 Patch

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a effettuare installazione e disinstallazione delle patch tramite prassi note.

20.6 Protezione dei dati di test

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a proteggere i dati di test tramite offuscamento o cifratura e di rendere gli stessi utilizzabili sono a personale autorizzato.

21. Change management

21.1 Formalizzazione del change management

Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare cambiamenti ai sistemi critici tramite prassi note o procedure formalizzate.

21.2 Notifica al Titolare

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a notificare il Titolare in merito a notevoli cambiamenti relativi alla *User Experience*.

22. Rapporti di lavoro

22.1 Prima dell'instaurazione del rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

22.2 Durante il rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i manager si assicurino che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni.

22.3 Conclusione o modifiche al rapporto di lavoro

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

23. Conformità

23.1 Conformità ai requisiti legali e contrattuali

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla *privacy* comunque idonee a consentire l'identificazione personale e la crittografia.

23.2 Revisione della sicurezza delle informazioni

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite *audit*) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle *policy* di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.

***

Funzione Privacy OPBG: privacy@opbg.net

Data Protection Officer: Angelo Loiacono - Piazza S. Onofrio n. 4 (Roma) – Tel. 06.6859.4018 -E-mail: dpo@opbg.net – Pec: dpo@pec.opbg.net