Bambino Gesù
FONDAZIONE

MODELLO ORGANIZZATIVO PRIVACY (MOP)

FONDAZIONE BAMBINO GESÙ ONLUS

Principali riferimenti:

Adozione	Disposizione del 15/12/2021
Titolare del Trattamento	Fondazione Bambino Gesù Onlus - Istituzione della Santa Sede Legale Rappresentante – Presidente del Consiglio Direttivo – Mariella Enoc
Codice Fiscale	97531780589
Sede legale	Roma, Passeggiata del Gianicolo, snc - c/o Villino Sion
Sede operativa	Roma, Via di Villa Pamphili, 100, Cap 00152
Sito web	www.fondazionebambinogesu.it
Contatti	(+39) 06.6859.2946 Mail: info.fond@fondbg.it Pec: fondazione.bambinogesu@pec.opbg.net

Il presente Modello Organizzativo Privacy di proprietà esclusiva della Fondazione Bambino Gesù Onlus - che sostituisce integralmente ogni precedente in materia e può essere revocato o modificato dal titolare del trattamento, in persona del Presidente quale legale rappresentante della Fondazione - ha efficacia immediata.

Il MOP può essere diffuso per gli usi consentiti.

Il Presidente

Mariella Enoc

INDICE

DEFINIZIONI:

Regolamento (o "GDPR"): è il Regolamento Generale sulla Protezione dei Dati in sigla GDPR (in inglese General Data Protection Regulation), ufficialmente Regolamento (UE) 2016/679, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018.

Codice: è il Codice per la protezione dei dati personali, emanato con il Decreto legislativo 30 giugno 2003, n. 196, in vigore dal 1º gennaio 2004 (da ultimo modificato dal Decreto legislativo 10 agosto 2018, n. 101).

Garante: è il Garante per la protezione dei dati personali, un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento (UE) 2016/679 (art. 51).

Diritto alla protezione dei dati personali: è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Appartiene alle persone fisiche viventi ed è un diritto autonomo rispetto al diritto alla riservatezza. Garantisce infatti all'individuo (Interessato) l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati. Tale diritto è oggi tutelato, in particolare, dal GDPR e dal Codice.

Interessato: è la persona fisica cui si riferiscono i dati personali.

Titolare del trattamento (o "Titolare"): 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.

Contitolare: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento.

Responsabile interno del trattamento (o "Responsabile interno"): dirigente al quale è affidata la responsabilità di presiedere l'applicazione del Regolamento nella propria area di competenza.

Responsabile esterno del trattamento (o "Responsabile esterno"): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Persona autorizzata (o "autorizzato"): la persona fisica che effettua materialmente operazioni di trattamento sui dati personali sotto l'autorità diretta del Titolare o del Responsabile interno ovvero esterno.

Responsabile della protezione dei dati (o "Data Protection Officer" o "DPO"): la persona fisica o giuridica (interna o esterna all'Organizzazione) la cui funzione è quella di supportare il Titolare del trattamento ovvero il Responsabile interno del trattamento nell'osservare, valutare e regolare la gestione del trattamento di dati personali (e dunque la loro protezione), affinché questi siano trattati nel rispetto della normativa applicabile, fungendo da punto di contatto e cooperando con l'autorità di controllo per questioni connesse al trattamento.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati soggetti a trattamento speciale ("categorie particolari di dati personali" o "dati particolari", già "dati sensi-bili"): dati che rivelano l'origine razziale o etnica; le opinioni politiche; le convinzioni religiose o filosofiche; l'appartenenza sindacale; dati relativi alla vita sessuale o all'orientamento sessuale della persona.

Dati relativi alla salute: sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compre- sa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dato giudiziario: è il dato personale idoneo a rivelare i provvedimenti giudiziari penali ed amministrativi in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.

Dati identificativi: dati personali che permettono l'identificazione dell'interessato.

Dato anonimo: dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Registro delle attività di trattamento (o "Registro dei trattamenti" o "Registro"): è un documento (cartaceo e/o digitale) di censimento e analisi dei trattamenti effettuati dal Titolare o dal Responsabile esterno. In quanto tale, il Registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Trattamento di dati personali: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di strumenti elettronici, 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 distru-zione.

Trattamento a rischio: trattamento di dati personali suscettibile di cagionare un danno fisico, materiale o mora- le in particolar modo se il trattamento comporta discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale importante. Viene inoltre considerato trattamento particolarmente a rischio il trattamento di dati sensibili, la valutazione della personalità, preferenze ed interessi personali, affidabilità o comportamento. Infine è trattamento a rischio il trattamento di una notevole quantità di dati personali e un vasto numero di interessati.

Principio di non eccedenza e di minimizzazione: utilizzo solo di dati sufficienti al perseguimento dei legittimi fini dichiarati e non eccedenti i fini stessi.

Principio di esattezza: obbligo del titolare di agire sui dati inesatti rispetto alla finalità dichiarate, di garantire e verificare l'esattezza, aggiornamento e la completezza dei dati trattati, rettificando con tempestività le anomalie riscontrate.

Misure di garanzia: misure che, in base a quanto previsto all'art. 2 septies del Codice, sono disposte dal Garante a tutela del trattamento dei dati genetici, biometrici e relativi alla salute e individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati.

Misure di sicurezza o di protezione: Complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dalla norma.

Pseudonimizzazione: trattamento di dati personali a seguito del quale i dati personali stessi non possono più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, separatamente conservate e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non sia- no attribuiti a una persona fisica identificata o identificabile.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per- sonali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Strumenti elettronici: elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica: insieme degli strumenti elettronici e delle procedure di verifica anche indiretta dell'identità.

Credenziali di autenticazione o di accesso: dati e dispositivi in possesso di una persona da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Profilo o livello di autorizzazione: insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione: insieme di strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Analisi del rischio: utilizzo sistematico di informazioni per identificare le cause e stimare il rischio.

Tracciabilità: grado in cui i dati hanno attributi che forniscono una registrazione degli accessi ai dati e a tutte le modifiche effettuate ai dati in un contesto di utilizzo specifico.

Paese terzo: Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) ovvero un'organizzazione internazionale.

1 FINALITÀ E AMBITO D'APPLICAZIONE

1.1. FINALITÀ

Il presente documento rappresenta il Modello Organizzativo Privacy (di seguito "MOP") della Fondazione Bambino Gesù Onlus (di seguito "**Fondazione**"), predisposto per rispondere alle disposizioni del Regolamento (UE) 2016/679 (di seguito "GDPR") in merito al trattamento dei dati personali.

Il MOP è uno degli strumenti adottati dalla Fondazione per l'applicazione della normativa in materia di protezione dei dati personali, stabilisce le politiche e le misure organizzative/procedimentali per garantire che i Dati Personali:

a) siano acquisiti e trattati su idonea e pertinente base giuridica per scopi determinati, espliciti e legittimi;

b) siano trattati solo per le finalità proprie della Fondazione e in maniera non eccedente le predette finalità;

c) siano trattati nel rispetto dei diritti e della dignità degli interessati;

d) siano protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati;

e) siano comunicati legittimamente all'interno e all'esterno della Fondazione.

Il MOP, inoltre, ha la finalità di fornire supporto al Responsabile interno e all'autorizzato che svolgono operazioni di trattamento di dati personali negli ambiti di attività della Fondazione.

Tutte le risorse operanti all'interno della Fondazione hanno l'obbligo di garantirne la corretta applicazione, per gli ambiti di rispettivo presidio, garantendo così il rispetto della normativa sulla sicurezza dei dati personali, con espressa e non esclusiva attenzione al corretto impiego delle risorse informatiche.

Il MOP ha valenza regolamentare.

1.2. AMBITO D'APPLICAZIONE DELLE PRESENTI DIRETTIVE

Questo documento è vincolante per tutti i soggetti che prestano attività lavorativa e collaborativa in qualsiasi forma presso la Fondazione e, pertanto, dipendenti, lavoratori interinali, soggetti che svolgono prestazioni occasionali, lavoratori autonomi che ricoprano incarichi nell'assetto organizzativo e volontari ("Personale").

1.3. RIFERIMENTI NORMATIVI E DOCUMENTALI

Regolamento (UE) 2016/679;

Decreto Legislativo 196/2003;

Decreto Legislativo 101/2018;

Provvedimenti, pareri e linee guida del Garante;

Decreto Legislativo 81/2008 e l'ulteriore normativa applicabile in materia di salute e sicurezza sul lavoro;

Decreto Legislativo D. Lgs. 101/2020.

Per tutte le definizioni non contemplate, si fa riferimento a quelle contenute nel Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).

Per tutti i principi generali e particolari si fa riferimento a quelli contenuti nel GDPR e nel D. Lgs. 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali come novellato dal D.Lgs. 10 agosto 2018, n. 101, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; si fa riferimento inoltre ai Provvedimenti Generali ed alle Autorizzazioni Generali emanati dall'Autorità Garante per la Protezione dei dati personali.

1.4 CONTESTO E AMBITO OPERATIVO

La storia e la genesi comune della Fondazione e dell'Ospedale Pediatrico Bambino Gesù (di seguito "**Ospedale**" o "**OPBG**"), collocati nel medesimo alveo istituzionale della Santa Sede e del relativo corredo di valori e principi, opera anche a valere per una stringete e continua collaborazione, che peraltro costituisce la finalità istituzionale di supporto per la Fondazione a beneficio delle attività dell'Ospedale.

In tal ottica va letto il complesso di relazioni e interazioni funzionali ed operative, di collaborazione e gestione comune e sinergica di condivisione di spazi, sedi e servizi, di aspetti logistici, tecnici, tecnologici, informatici, di sicurezza, di comunicazione e di supporto che legano la Fondazione con l'Ospedale Pediatrico Bambino Gesù, e che trovano, nel presente documento, specifici riferimenti a servizi e ambiti di gestione.

2 TRATTAMENTI DI DATI PERSONALI

2.1. LA FONDAZIONE BAMBINO GESÙ ONLUS

La Fondazione, senza mai perseguire logiche di profitto, supporta l'Ospedale Pediatrico Bambino Gesù, impegnandosi ad assicurare risorse economiche da utilizzare per tutte le attività clinico-assistenziali in ambito pediatrico, con attenzione anche verso coloro ai quali l'accesso alle cure non sempre è garantito con pregiudizio della dignità umana e spirituale; il tutto perseguendo quindi finalità solidaristiche e di particolare rilevanza sociale.

Nel 1996, per atto del Papa Giovanni Paolo II, nasce la Fondazione "Cari Bambini", dedicata a sostenere l'attività di assistenza ospedaliera dei bambini dell'Ospedale Pediatrico Bambino Gesù, fondato nel 1869 e oggi Istituto di Ricovero e Cura a Carattere Scientifico (I.R.C.C.S.). Il 4 settembre 2000 la Fondazione acquisisce un nuovo statuto e la denominazione di "Fondazione Bambino Gesù".

La Fondazione, con sede nello Stato della Città del Vaticano, ha concretizzato la sua operatività nel territorio italiano mediante l'istituzione di una sede secondaria che ha consentito alla medesima il perseguimento delle proprie finalità statutarie per il sostegno delle iniziative umanitarie a supporto dell'attività assistenziale e di ricerca svolta dall'Ospedale Pediatrico Bambino Gesù e di aiuto ai bambini bisognosi di assistenza ospedaliera non fruenti del Servizio Sanitario Nazionale.

Dal 2008, con l'istituzione della sede secondaria, la Fondazione è stata iscritta nel Registro delle persone giuridiche presso la Prefettura di Roma e nell'Anagrafe delle ONLUS presso la Direzione Regionale Lazio con la denominazione attuale di Fondazione Bambino Gesù Onlus.

Nel novembre 2015, la Fondazione è stata completamente rinnovata nel suo Consiglio Direttivo che ha approvato il nuovo Statuto orientato a una trasparente operatività dell'Ente.

Le attività economiche della Fondazione sono soggette al Controllo del Collegio dei revisori. Il bilancio della Fondazione è certificato dalla società di revisione esterna.

Lo scenario normativo e operativo si colloca nell'alveo di riferimento della Santa Sede - Stato della Città del Vaticano e, per quanto di ragione e applicabile, nella legislazione italiana di settore.

Come da Statuto, la Fondazione non ha fini di lucro e persegue finalità di solidarietà sociale mediante la promozione e il sostegno dell'attività di ricerca scientifica di particolare interesse sociale dell'"Ospedale Pediatrico Bambino Gesù" in ambito sanitario e delle attività a essa strumentali, connesse, inerenti o dipendenti.

2.1.1. L'adozione, l'aggiornamento e l'adeguamento del MOP

Il Presidente, quale legale rappresentante della Fondazione, è l'organo competente per l'adozione, l'aggiornamento e l'adeguamento del MOP che deve essere oggetto di aggiornamento o adeguamento ogni qual volta se ne ravvisi la necessità o l'opportunità e comunque in conseguenza di circostanze che attengano a fatti quali:

- modifiche del quadro normativo di riferimento che abbiano impatto sui Processi o che abbiano ad oggetto l'introduzione di nuovi adempimenti;
- significative modificazioni dell'assetto organizzativo o delle deleghe;
- modifiche delle attività che abbiano impatto sui Processi;
- valutazioni di inadeguatezza all'esito dei controlli eseguiti.

2.2. TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento dei dati è la Fondazione Bambino Gesù Onlus, nella persona del Presidente Mariella Enoc, quale legale rappresentante.

Il Titolare del Trattamento è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR quali liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate al fine di garantire ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Il Titolare, inoltre, provvede a:

a) nominare il Responsabile della protezione dei dati (RPD) – Data Protection Officer (DPO), ove previsto;

b) designare i Responsabili interni del trattamento;

c) nominare quali Responsabili esterni del trattamento (ai sensi dell'articolo 28 GDPR) i soggetti pubblici o privati affidatari di attività e servizi per conto della Fondazione;

d) predisporre l'elenco dei Responsabili interni del trattamento delle strutture in cui si articola l'organizzazione della Fondazione;

e) predisporre il piano triennale degli interventi sviluppato tenuto conto dell'analisi dei rischi effettuata e il cui giudizio sintetico è riportato all'interno del Registro delle attività di trattamento, soggetto a verifica e revisione annuale.

Il Titolare, nell'esercizio delle predette attività, si avvale del supporto e della prospettazione tecnica del Responsabili interno, e all'occorrenza di supporto consulenziale specialistico e indipendente esterno, ovvero, del DPO.

2.3. CONTITOLARI DEL TRATTAMENTO

Nei rapporti con terze parti che comportino la condivisione di dati e il trattamento degli stessi da parte di terzi, la decisione se procedere con la stipula di un accordo di contitolarità o con la nomina di un Responsabile esterno del trattamento o attraverso titolarità autonome è riservata al Responsabile interno, sentito il DPO che, in fase di valutazione preliminare della documentazione contrattuale, formulerà la relativa proposta.

Nel caso di definizione di un accordo di contitolarità si deve procedere con il Contitolare a determinare congiuntamente le finalità e la modalità del trattamento.

L'accordo di riparto (ovvero "accordo di contitolarità") è sottoscritto nel rispetto dei poteri di firma.

Nell'accordo con il Contitolare devono essere definite e chiaramente distinte le responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa vigente e dal MOP, in relazione al trattamento o alla parte di trattamento da ciascuno posta in essere con particolare riguardo all'esercizio dei diritti dell'interessato e in generale ai rapporti di ciascuno con l'interessato.

Indipendentemente dalle disposizioni dell'accordo della Fondazione con i Contitolari, il Responsabile del trattamento nominato dalla Fondazione assicura, per quanto nella loro materiale possibilità, l'esercizio dei loro diritti da parte degli interessati ed eventualmente segnala al DPO della Fondazione eventuali inadempienze del Contitolare.

2.4. RESPONSABILI ESTERNI DEL TRATTAMENTO

Il Responsabile esterno del trattamento, ai sensi dell'art. 28 del GDPR, è un soggetto esterno che esegue, in base a un contratto o altro atto giuridico, trattamenti di dati personali per conto del Titolare e ne risponde in solido in caso di inadempienze. Al Responsabile esterno spettano tutti i compiti del Titolare all'interno della propria organizzazione (registro dei trattamenti, eventuale nomina del Responsabile della Protezione Dati, nomina degli autorizzati, formazione, ecc.).

Nel caso di trasferimento di dati verso un Paese terzo è obbligatorio informare di ciò l'Interessato e il Titolare deve verificare che il Responsabile esterno assicuri un'adeguata protezione dei dati.

La nomina di un Responsabile esterno deve essere contenuta in un contratto tra il Responsabile così nominato e la Fondazione ovvero formalizzata in un atto di nomina da allegare al contratto.

Il contratto deve indicare e stabilire:

a) la durata del trattamento;

b) la natura e la finalità del trattamento;

c) il tipo di dati personali e le categorie di interessati;

d) gli obblighi e i diritti della Fondazione.

Il contratto deve, altresì, prevedere l'impegno del Responsabile esterno:

a) a trattare i dati personali seguendo le istruzioni specifiche e particolari della Fondazione;

b) a trattare i dati personali, anche di natura particolare e sanitaria, esclusivamente per le finalità previste dal contratto;

c) a compilare e tenere aggiornato il proprio registro dei trattamenti rendendolo accessibile alla Fondazione su richiesta specifica della stessa;

d) a nominare le persone autorizzate al trattamento e garantire che i dati trattati siano portati a conoscenza soltanto del personale autorizzato del trattamento salvo che sia diversamente previsto da un obbligo inderogabile di legge;

e) a garantire e documentare che le persone incaricate del trattamento dei dati personali si siano impegnate alla riservatezza ovvero abbiano un obbligo legale o deontologico alla riservatezza;

f) a garantire e documentare l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio connesso al trattamento quali, a titolo esemplificativo, la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la

disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

g) a vigilare affinché ciascun dato personale venga trattato per i soli fini per i quali è stato raccolto;

h) a vigilare affinché i documenti contenenti dati personali vengano custoditi in modo da non essere accessibili a persone non autorizzate al trattamento;

i) a garantire i diritti degli interessati ovvero a provvedere direttamente a soddisfare eventuali richieste degli stessi che siano manifestazione di un diritto loro attribuito dalla normativa vigente;

j) a cancellare o restituire alla Fondazione tutti i dati personali alla scadenza del contratto salvo che vi sia un obbligo stabilito da una diposizione inderogabile di legge che preveda la conservazione dei dati da parte del Responsabile esterno;

k) a consentire le attività di audit, comprese le ispezioni, da parte della Fondazione o da un altro soggetto da questo incaricato.

Ogni contratto contenente la nomina di Responsabile esterno deve essere trasmesso al DPO.

2.5. RESPONSABILI INTERNI DEL TRATTAMENTO (OVVERO DESIGNATI)

Trattano i dati per conto del Titolare e vengono designati con un atto di nomina.

Hanno il compito di individuare, nominare ed istruire per iscritto, nell'ambito della loro attività, i soggetti autorizzati al trattamento dei dati, assicurandosi che questi rispettino quanto stabilito nel MOP nonché dalla normativa vigente.

In particolare, ogni Responsabile interno del trattamento dovrà garantire:

- l'adozione di idonee misure per assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale;
- la segnalazione in merito alla opportunità/necessità di creare un nuovo trattamento nel caso in cui sia necessario avviare un nuovo servizio/attività che comporti il trattamento di dati personali;
- la correttezza, l'esattezza e la completezza di dati personali oggetto del trattamento;
- la nomina delle persone autorizzate al trattamento dei dati personali;
- che non siano trasmesse e non sia consentito l'accesso ai Dati Personali a persone non autorizzate al trattamento;
- che i dati, di cui è responsabile, siano trasmessi e sia consentito l'accesso solo dopo aver verificato l'adozione di tecniche di protezione appropriate ed eventualmente stabilite nel MOP (es. la pseudonimizzazione, la cifratura, l'anonimizzazione dei dati personali) o, in assenza, da istruzioni specifiche della Fondazione o da norme di legge;
- la vigilanza sulle persone autorizzate affinché operino conformemente alle disposizioni normative, regolamentari e alle istruzioni loro impartite, ivi compresa l'adozione e l'effettivo utilizzo della modulistica comprendente l'informativa di cui agli artt. 13 e 14 del GDPR, che deve sempre essere resa agli Interessati cosi come il consenso al trattamento dei dati personali che deve essere raccolto nei casi in cui sia previsto dalla legge;

- garantire che chiunque tratti i dati personali abbia ricevuto e riceva una formazione adeguata;
- la costante collaborazione con il DPO.

2.6. AUTORIZZATI AL TRATTAMENTO

Gli Autorizzati al trattamento sono designati, a gruppi o singolarmente, dal Responsabile interno del trattamento.

Le responsabilità sono dettagliate per iscritto nella lettera di nomina. Ferme le attribuzioni del Titolare del trattamento è comunque compito del Responsabile interno individuare, all'interno del proprio ambito di presidio, gli autorizzati al trattamento, intesi come persone fisiche autorizzate a compiere operazioni di trattamento e fornire loro adeguate istruzioni.

Il Personale preposto ad un determinato servizio che implichi il trattamento di dati personali, ovvero che sia assegnato ad una mansione anche non ricorrente ma che implichi il trattamento di dati personali, deve essere formalmente autorizzato al trattamento dei dati personali con apposita nomina. L'atto di nomina deve individuare l'ambito del trattamento consentito, in stretta relazione con le attività previste nell'articolazione organizzativa di competenza, anche se solo funzionalmente, alla qualifica ricoperta e alle mansioni assegnate alla persona autorizzata al trattamento.

L'atto di nomina deve essere aggiornato in occasione del mutamento delle mansioni o del profilo funzionale della persona autorizzata anche a seguito di trasferimento all'interno della medesima articolazione organizzativa ed è efficace fino a revoca ovvero fino alla cessazione del rapporto di collaborazione con la Fondazione e deve essere reiterato, o modificato, dal Responsabile interno del trattamento in presenza di ogni rinnovo o di un nuovo affidamento di mansioni all'interno della Fondazione.

In ogni caso il Responsabile interno del trattamento deve verificare gli atti di nomina delle persone autorizzate al trattamento con cadenza annuale per eventuali adeguamenti riguardanti le fonti normative o regolamentari, le mutate esigenze, le modifiche procedurali, i mutamenti dei ruoli o le cessazioni dal servizio.

La persona autorizzata al trattamento, nello svolgimento delle operazioni strettamente connesse all'adempimento delle sue funzioni, deve attenersi al MOP e alle istruzioni impartite dal Responsabile interno del trattamento da cui dipende in occasione della progettazione di nuovi trattamenti.

Le persone autorizzate al trattamento devono comunque assicurare che i dati personali:

a) siano raccolti e registrati per scopi determinati, espliciti e legittimi, conformemente al consenso prestato dall'interessato o alle finalità coerenti con la diversa base giuridica del trattamento individuata dal MOP o a seguito di DPIA;

b) siano esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti rispetto al conseguimento delle finalità per le quali il dato viene raccolto e, ove si tratti di dati sensibili, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;

c) siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2.7. RESPONSABILE DELLA PROTEZIONE DEI DATI (O DATA PROTECTION OFFICER)

E' la persona fisica o giuridica (interna o esterna all'Organizzazione) la cui funzione è quella di supportare il Titolare del Trattamento e il Responsabile interno del Trattamento nell'osservare, valutare e regolamentare la gestione del trattamento dei dati personali, affinché questi siano trattati nel rispetto della normativa applicabile.

Opera in autonomia e coopera con l'autorità di controllo per tutto ciò che riguarda il trattamento dei dati.

Nell'esecuzione dei propri compiti il DPO provvede:

- alla raccolta di informazioni per individuare i trattamenti svolti;
- alla verifica che i trattamenti svolti siano conformi alla normativa vigente;
- all'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile interno sull'adeguatezza dei presidi tecnici, organizzativi e procedurali messi in atto per la tutela dei diritti degli interessati;
- a prestare la propria consulenza alla Fondazione in caso di esercizio da parte degli Interessati dei diritti loro riconosciuti dalla legge;
- alla gestione dei rapporti con le Autorità pubbliche di vigilanza.
- I Responsabili interni del trattamento devono coinvolgere il DPO fin dalla fase di progettazione di attività e processi che comportino il trattamento di dati personali.

In particolare, il DPO dovrà essere consultato sulle seguenti tematiche:

- se condurre o meno una valutazione di impatto e di rischio (DPIA);
- se l'analisi del rischio (DPIA) è stata condotta correttamente e se le conclusioni raggiunte (procedere o meno con il trattamento) siano conformi alla normativa vigente;
- se condurre l'analisi del rischio (DPIA) con le risorse interne o esternalizzandola;
- quali tutele adottare, comprese misure tecniche e organizzative, per ridurre al minimo rischi per i diritti degli interessati;
- se il Registro delle attività di trattamento sia correttamente tenuto;
- se eventuali rischi residui debbano prevedere una consultazione preventiva con l'Autorità Garante

2.8 MODALITÀ DEL TRATTAMENTO E CONSERVAZIONE DEI DATI

Il trattamento dei dati personali è eseguito da parte del Titolare nel rispetto di quanto previsto dalla vigente normativa in materia di protezione dei dati personali. Il Titolare effettua il trattamento dei dati personali mediante strumenti informatici e/o telematici e con modalità organizzative strettamente correlate al perseguimento delle finalità indicate nell' informativa, nonché adottando le misure di sicurezza opportune al fine di impedire l'accesso, la divulgazione, la modifica o la distruzione non autorizzata dei dati personali, la loro perdita e il loro utilizzo illecito e non corretto. La gestione e la conservazione dei dati personali acquisiti avverrà presso archivi o su server ubicati all'interno dell'unione europea di proprietà del Titolare e/o di società terze, nominate responsabili esterni del trattamento.

In relazione alle diverse finalità per i quali sono raccolti, i dati personali saranno conservati per il tempo strettamente necessario al conseguimento delle stesse e, in ogni caso, conformemente alle disposizioni normative vigenti in materia.

2.10 REFERENTI DEI SISTEMI INFORMATIVI DELL'OSPEDALE PEDIATRICO BAMBINO GESU'

I Sistemi Informativi dell'Ospedale Pediatrico Bambino Gesù, per gli ambiti di rispettiva competenza, garantiscono la gestione e manutenzione dei sistemi informatici, l'effettuazione ed il monitoraggio del

backup dei dati, nonché tramite società esterne per la manutenzione di alcune delle apparecchiature e dei dispositivi in uso alla Fondazione. Tali società sono formalmente impegnate a fronte di una nomina a Responsabile esterno (*ex* art. 28 GDPR) ad operare nel rispetto della normativa vigente e a garantire la segretezza delle informazioni riservate a cui dovessero accedere nell'esecuzione del proprio lavoro, nonché ad attestare per iscritto la conformità degli interventi effettuati sul sistema.

2.11 TRASFERIMENTO DI DATI ALL'ESTERO

I dati personali potranno essere trasferiti all'estero, in conformità a quanto previsto dalla normativa vigente, anche in Paesi non appartenenti all'unione europea solo se il trasferimento in tali paesi, è garantito da decisioni di adeguatezza stabilite dalla commissione Europea ed è effettuato in modo da fornire garanzie appropriate e opportune ai sensi degli art. 46 o 47 o 49 del GDPR.

2.12 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

2.12.1. Trattamenti svolti dalla Fondazione in qualità di Titolare

Il Registro delle Attività di Trattamento raccoglie le informazioni di tutti i trattamenti svolti dalla Fondazione in qualità di Titolare e in qualità di Responsabile Esterno.

Il Registro delle attività di trattamento svolte dal Titolare del trattamento deve contenere le seguenti informazioni:

a) il nome ed i dati di contatto della Fondazione, del Rappresentante legale e/o del suo Delegato, del Responsabile interno;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un Paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il Registro è tenuto dal Titolare in forma telematica/cartacea presso la sede del Titolare ed è costantemente alimentato ed aggiornato da Personale all'uopo autorizzato.

2.12.2. Trattamenti svolti dalla Fondazione in qualità di Responsabile esterno

Obblighi analoghi a quelli previsti al paragrafo che precede gravano sulla Fondazione nel caso in cui venga designato Responsabile esterno del trattamento ai sensi dell'articolo 28 del GDPR. In tale Registro devono essere inseriti tutti i trattamenti di dati che la Fondazione dovesse svolgere in qualità di Responsabile esterno del trattamento nominato da altro Titolare.

In particolare, il Registro delle categorie di attività trattate dalla Fondazione in qualità di Responsabile esterno dovrà contenere le seguenti indicazioni:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e del DPO;

b) le categorie dei trattamenti effettuati per conto del titolare del trattamento;

c) la durata del trattamento;

d) l'eventuale trasferimento di dati personali verso un Paese terzo od una organizzazione internazionale;

e) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il Registro è tenuto dall'ente presso i propri uffici.

2.13. ANALISI DEI RISCHI

La Fondazione adotta una modalità di valutazione dei rischi stringente anche in applicazione di un modus operandi improntato al miglioramento continuo nella gestione dei dati personali per il trattamento del rischio relativo alla sicurezza delle informazioni, in funzione dell'obiettivo specifico dell'organizzazione di tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati. Conseguentemente i rischi valutati sono focalizzati sulla tutela dei diritti e delle libertà delle persone fisiche e non sui rischi per l'organizzazione stessa.

3 PROTEZIONE DEI DATI

3.1. ACQUISIZIONE DEI DATI PERSONALI

Un dato personale è acquisito dalla Fondazione quando viene ricevuto dal proprio Personale autorizzato al trattamento nell'esercizio delle proprie funzioni, in forma scritta (anche mediante mezzi informatici) o orale (anche mediante sistemi audio/video) ovvero quando viene acquisito in maniera automatica senza intervento umano e viene archiviato su qualunque supporto che ne consenta il successivo trattamento a qualunque fine.

I dati personali sono acquisiti direttamente dall'Interessato quando è l'Interessato medesimo, o chi ne abbia la rappresentanza, a trasmetterli alla Fondazione con qualsiasi mezzo e in qualsiasi forma, scritta o orale.

I dati non sono acquisiti dall'interessato quando sono già in possesso della Fondazione ovvero quando vengono forniti da un terzo a ciò debitamente autorizzato.

3.2. INFORMATIVA

Il rilascio agli Interessati dell'informativa è adempimento inderogabile, qualunque sia la base giuridica utilizzata per il trattamento dei dati personali, di conseguenza anche ove non necessario il consenso dell'interessato o di chi ne ha la rappresentanza.

Il Responsabile interno del trattamento deve assicurare che prima dell'acquisizione dei dati personali o contestualmente all'acquisizione degli stessi sia stata consegnata o comunque messa a disposizione degli interessati o di chi li rappresenta l'informativa sul trattamento dei dati personali.

Il rilascio dell'informativa all'interessato o a chi ne ha la rappresentanza ovvero l'indicazione allo stesso del luogo dove è possibile reperirla, può essere omesso solo nel caso in cui:

a) la Fondazione, e per essa il Responsabile interno del trattamento, sia nell'impossibilità di contattare l'interessato, ovvero, qualora, sentito il Titolare o all'esito dell'eventuale esecuzione di una DPIA, contattare gli interessati richieda uno sforzo sproporzionato rispetto al rischio di compromissione dei suoi diritti fondamentali;

b) qualora sia già stata resa in precedenza al medesimo interessato, sempre che alcuni elementi della stessa non siano cambiati in parallelo ad una corrispondente modifica del Registro dei trattamenti. In tale ultimo caso gli interessati devono essere informati dei soli cambiamenti intervenuti sempre che non ricorra una delle ipotesi di cui alle lett. a) e b) che precedono.

Il Responsabile interno del trattamento assicura che l'informativa sia trasparente, intelligibile per l'interessato e facilmente accessibile e veicolata da un linguaggio chiaro e semplice evitando per quanto possibile termini tecnici.

Nei trattamenti che richiedono l'espletamento di una DPIA l'informativa è redatta all'esito della stessa e secondo le indicazioni risultanti dalla valutazione.

In caso di rapporti di contitolarità l'informativa è fornita salvo che l'accordo tra la Fondazione e il contitolare preveda:

a) che l'informativa sia resa da quest'ultimo;

b) che il contitolare renda informativa separata per i trattamenti o parte di essi da questo posti in essere.

I contenuti dell'informativa sono forniti anche con riferimento ai dati, ai trattamenti e alle finalità che ricadono in base agli accordi sotto la responsabilità del Contitolare.

In ogni caso, l'informativa contiene una descrizione sintetica dell'accordo tra la Fondazione e il Contitolare.

Il Responsabile interno, definisce in allegato all'accordo un modello di informativa in relazione ai trattamenti oggetto dell'accordo medesimo.

3.2.1. Informativa sulla registrazione audio/video

In caso di registrazioni di immagini riconducibili alle attività della Fondazione, compresi eventi che vedono la presenza di personaggi del mondo dello sport, dello spettacolo, e più in generale della televisione e dei media dovrà essere fornita agli Interessati (pazienti, genitori ecc..) preventivamente una informativa specifica, redatta in occasione dell'evento, comprensiva di modulo di consenso a poter effettuare la registrazione delle immagini.

In assenza del consenso, non sarà possibile in nessun caso procedere con l'acquisizione delle immagini né video né audio.

3.2.2. Informativa sull'utilizzo di cookies nel sito web

L'informativa sintetica deve immediatamente comparire in primo piano in un banner di idonee dimensioni, ossia di dimensioni tali da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che si sta visitando contenente le seguenti indicazioni:

a) che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;

b) che il sito consente anche l'invio di cookie "terze parti" (laddove ciò ovviamente accada);

c) il link all'informativa estesa, ove vengono fornite indicazioni sull'uso dei cookie tecnici e analytics, viene data la possibilità di scegliere quali specifici cookie autorizzare;

d) l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie;

e) l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie.

Il banner, oltre a dover presentare dimensioni sufficienti a ospitare l'informativa, seppur breve, deve essere parte integrante dell'azione positiva nella quale si sostanzia la manifestazione del consenso dell'utente. Il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell'utente (appunto attraverso la selezione di un elemento contenuto nella pagina sottostante il banner stesso). È necessario in ogni caso che dell'avvenuta prestazione del consenso dell'utente sia tenuta traccia mediante apposito cookie tecnico.

La presenza di tale "documentazione" delle scelte dell'utente consente poi di non riproporre l'informativa breve alle successive visite del medesimo utente.

L'informativa estesa deve contenere tutti gli elementi previsti dalla normativa vigente, descrivere in maniera specifica e analitica le caratteristiche e le finalità dei cookie installati dal sito e consentire all'utente di selezionare/deselezionare i singoli cookie. Deve essere raggiungibile mediante un link inserito

nell'informativa breve, come pure attraverso un riferimento su ogni pagina del sito, collocato in calce alla medesima.

3.2.3. Informativa in caso di acquisizione dei dati da soggetti terzi

Qualora i dati siano acquisiti da terzi, il Responsabile interno del trattamento deve assicurarsi che, prima di avviare il trattamento, sia stata fornita agli interessati l'informativa estesa ovvero il link al sito della Fondazione da cui acquisirla.

Ove tale informativa non sia stata resa, il Responsabile interno del trattamento deve provvedervi eventualmente facendone istanza al Titolare alternativamente:

a) entro trenta giorni da quando i dati sono stati acquisiti;

b) nel caso in cui i dati personali, anche all'esito del trattamento, siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;

c) nel caso in cui i dati, anche all'esito del trattamento, debbano essere comunicati ad altro destinatario, prima di detta comunicazione dei dati personali.

L'obbligo di rendere l'informativa non sussiste:

a) qualora i dati siano acquisiti a fini di ricerca scientifica o a fini statistici, e nella misura in cui l'onere di informativa possa impedire o pregiudicare gravemente tale finalità di trattamento;

b) quando l'acquisizione dei dati personali ovvero la loro comunicazione alla Fondazione siano previsti da un obbligo di legge;

c) qualora le persone autorizzate al trattamento siano comunque obbligate ad osservare il segreto professionale su quei dati o trovi applicazione altro obbligo di segretezza previsto per legge.

3.3. CONSENSO

3.3.1. Modalità di raccolta del consenso nei locali della Fondazione

Le persone autorizzate al trattamento devono raccogliere il consenso al trattamento dei dati procedono secondo le seguenti modalità:

a) devono verificare l'identità dell'interessato chiedendogli di esibire un documento di riconoscimento in corso di validità e riscontrare la corrispondenza dei dati con quanto dichiarato nel modello;

b) prima di consegnare il modulo per il consenso, qualora necessario, la persona autorizzata al trattamento deve verificare che lo stesso non risulti precompilato in nessuna sua parte;

c) nel caso gli interessati siano minori, le persone autorizzate al trattamento devono verificare che il modello per la raccolta del consenso sia stato debitamente compilato nella parte in cui chi presta il consenso debba dichiarare di avere la responsabilità genitoriale o essere il legale rappresentante ovvero un loro delegato;

d) in ogni caso le persone autorizzate al trattamento devono verificare che sia stata sottoscritta la dichiarazione di presa visione dell'informativa;

e) il consenso deve essere rilasciato in forma scritta utilizzando l'apposito modulo predisposto dalla Fondazione e deve riguardare in maniera separata e distinta il trattamento dei dati personali;

f) la persona autorizzata al trattamento deve assicurare la conservazione del modulo relativo al consenso per tutta la durata del trattamento e deve assicurarsi che lo stesso sia a disposizione delle articolazioni organizzative che eseguono i trattamenti per i quali il consenso è stato prestato.

3.3.2. Esclusione del consenso

Anche a prescindere dall'esecuzione di una DPIA possono essere raccolti e trattati i dati personali senza necessità di consenso dell'interessato:

a) nella gestione del rapporto di lavoro trovando il trattamento fondamento nel relativo contratto e purché sia a questo allegata la relativa informativa o la stessa sia stata comunicata al dipendente in caso di nuovo trattamento;

b) per la difesa della Fondazione in giudizio e di fronte ad autorità amministrative;

c) in tutti i procedimenti volti ad adempiere agli obblighi normativi e/o procedurali di comunicazione di dati personali connessi al collega mento tra Fondazione e Istituzioni o Enti o Autorità.

I trattamenti di dati personali effettuati nell'ambito della gestione del rapporto di lavoro ma non rientranti nelle obbligazioni di natura contrattuale né negli obblighi di natura normativa, richiedono la preventiva acquisizione del consenso esplicito dell'interessato necessario per ciascuna delle finalità specifiche ulteriori.

3.3.3. Il consenso prestato per via telematica in relazione ai servizi prestati dalla Fondazione

L'accesso ai servizi on-line della Fondazione deve essere consentito solo a utenti registrati ovvero in possesso di altri strumenti di identificazione analoghi, nel tempo eventualmente predisposti dalla Fondazione.

La registrazione deve poter avvenire solo a titolo personale mediante emissione di codici identificativi e chiavi di accesso univoche e deve essere confermata mediante procedura che preveda l'invio di una e-mail all'indirizzo dichiarato nel form di registrazione dell'interessato con indicazione di un link.

Qualora per il tipo di servizio richiesto sia necessario comunicare in sede di accesso ai servizi telematici i dati relativi ai minori, gli esercenti la responsabilità genitoriale al momento della registrazione devono spuntare la casella nella quale dichiarano di essere gli esercenti la responsabilità genitoriale su uno o più minori.

Al fine di assicurare una corretta acquisizione del consenso, qualora necessario:

a) nessuna delle caselle deve essere preimpostata;

b) l'interessato deve aver selezionato la casella di presa visione dell'informativa che deve essere distinta da quella per la prestazione del consenso;

c) le caselle del consenso devono avere funzione esclusiva e devono essere distinte per ogni trattamento avente finalità diversa;

d) la mancata prestazione del consenso deve impedire l'accesso al servizio on-line esclusivamente se è omesso in relazione ai dati che sono necessari all'esecuzione del servizio medesimo.

3.3.4. Consenso prestato mediante collegamento audio

In caso di accesso a servizi per il tramite di collegamento audio, il consenso qualora necessario può essere prestato:

a) mediante voce preregistrata che avvisi l'interessato che proseguendo nella conversazione presta il consenso al trattamento dei dati;

b) mediante la richiesta di digitare un numero sulla tastiera per esprimere il consenso al trattamento dei dati.

3.4. PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

Il Responsabile interno del trattamento nell'organizzazione e nella gestione delle funzioni della Fondazione, adotta le politiche generali per la tutela della riservatezza degli interessati di cui al presente MOP.

Qualora per motivi di migliore organizzazione e gestione dei servizi sorga la necessità di discostarsi dalle politiche descritte nel presente documento, il Responsabile interno del trattamento deve consultare il DPO e valutare congiuntamente con questi se, in ragione del rischio elevato per i diritti degli interessati, debba preventivamente procedersi con una DPIA.

4 STRUMENTI E SICUREZZA

4.1. POLITICHE GENERALI PER IL TRATTAMENTO DI DATI IN FORMA CARTACEA

L'archiviazione e la catalogazione dei documenti deve essere organizzata in maniera da permettere la pronta reperibilità e l'identificazione dell'interessato, al fine di consentire l'esercizio dei propri diritti da parte di quest'ultimo.

Gli atti e i documenti contenenti dati personali, affidati alle persone autorizzate al trattamento per lo svolgimento dei relativi compiti, devono essere utilizzati assicurandosi che agli stessi non abbia accesso altro personale della Fondazione non coinvolto nel trattamento, ovvero a visitatori e terze parti.

Le singole fasi di lavoro e la condotta da osservare devono evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

Pertanto:

a) i documenti devono essere conservati in archivi chiusi accessibili solo al personale autorizzato al trattamento che ne comporti l'utilizzo;

b) il prelievo e la restituzione di atti e documenti dall'archivio deve essere annotato in apposito registro ove vengano riportati i dati della persona autorizzata al trattamento, la data del prelievo e quella della riconsegna;

c) i medesimi atti e documenti possono essere presi dall'archivio e detenuti presso le postazioni di lavoro delle persone autorizzate al trattamento a ciò legittimati, che devono provvedere alla loro custodia. Alla cessazione delle attività di trattamento devono essere restituiti all'archivio;

d) tutte le operazioni di trattamento devono essere effettuate considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

e) i documenti contenenti dati personali non devono essere portati fuori dalla Fondazione, salvo che l'asporto sia necessario per il perseguimento delle finalità connesse al trattamento per il quale sono stati raccolti. In tali casi dovrebbe portarsi all'esterno una copia dell'atto e non l'originale. Ove ciò non sia possibile deve lasciarsi in archivio una copia dell'atto o del documento, ovvero provvedere alla digitalizzazione dello stesso e alla sua archiviazione informatica;

f) in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro, si devono porre in essere tutte le misure necessarie affinché altri dipendenti non autorizzati al medesimo trattamento, visitatori o terzi, non possano accedere ai dati personali;

g) la postazione di lavoro deve essere utilizzata in modo esclusivo da un solo utente e protetta, evitando che terzi possano accedere ai dati che si stanno trattando. Nella turnazione del personale può consentirsi l'avvicendamento di più persone nella stessa postazione, purché tutte autorizzate al medesimo trattamento;

h) qualora si ricevano alla propria postazione di lavoro dipendenti della Fondazione non autorizzati al trattamento, ovvero terze persone, e si tengano sulla propria scrivania cartelle e fascicoli, devono essere adottate misure di pseudonimizzazione mediante copertura, anche temporanea, dei dati identificativi dell'interessato riportati sul frontespizio dei documenti, dei fascicoli e delle cartelle. Si deve quindi inserire, a seconda delle necessità operative e organizzative, informazioni che non permettano di percepire l'identità dei soggetti interessati dal trattamento. In caso di allontanamento non devono essere lasciati sulla scrivania documenti contenenti dati personali, a meno che non si chiuda a chiave la porta della stanza;

i) gli atti e i documenti dei quali esiste un unico esemplare dovrebbero essere digitalizzati;

j) salvo che si tratti di copie, la distruzione di documenti deve essere preceduta dalla verifica che sia spirato il termine di conservazione come riportato nel Registro del trattamento in relazione alla categoria di riferimento avuto riguardo alla data di protocollo in entrata. Ove non si conosca la data di acquisizione del documento da parte della Fondazione deve aversi riguardo alla data in cui il documento è pervenuto all'interessato. Prima di gettare la documentazione nel cestino della carta si deve provvedere a renderne non comprensibile il contenuto ovvero procedere alla separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli e distruzione di quelli contenenti dati identificativi.

4.2. POLITICHE GENERALI PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Si specifica che le risorse informatiche aziendali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali.

Il personale autorizzato è tenuto a contattare il Responsabile interno e quindi la Funzione Sistemi Informativi dell'Ospedale prima di intraprendere qualsiasi attività tecnica e/o di sistema informativo al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ospedale e condivisi dalla Fondazione.

È vietata la connessione alla rete aziendale di qualsiasi dispositivo non preventivamente autorizzato dalla Funzione Sistemi Informativi dell'Ospedale.

4.3. POLITICHE GENERALI RELATIVE ALLA PROTEZIONE DEI DATI PARTICOLARI E ALLA CONDIVISIONE ALL'INTERNO DELLA FONDAZIONE

Nel contesto della ordinaria gestione dei dati per le attività della Fondazione, non si configura l'ipotesi di trattamenti di dati idonei a rivelare:

a) l'origine razziale o etnica;

b) le opinioni politiche;

c) le convinzioni religiose o filosofiche;

d) l'appartenenza sindacale;

e) dati genetici;

f) dati biometrici intesi a identificare in modo univoco una persona fisica;

g) dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona.

Ove comunque, detta eventualità dovesse presentarsi, il Responsabile interno può consentirne:

(i) la condivisione con altre funzioni della Fondazione;

(ii) l'impiego per un trattamento diverso da quello per il quale sono stati originariamente acquisiti;

(iii) la conservazione per un periodo eccedente il termine di conservazione del trattamento e in assenza di possibili o probabili, ulteriori futuri, trattamenti,

solo se, alternativamente:

a) il trattamento ulteriore senza applicazione delle misure di protezione è stato oggetto di consenso da parte dell'interessato;

In assenza la funzione ricevente si astiene dal trattamento;

b) i dati vengono sottoposti a procedure di anonimizzazione o pseudonimizzazione;

c) il trattamento ulteriore è stato oggetto di DPIA, nel qual caso la trasmissione avviene nel rispetto delle prescrizioni della DPIA. La funzione trasmittente deve verificare dal Registro dei trattamenti il documento di DPIA;

d) il dato deve essere trasferito alla funzione ricevente per consentirle di svolgere un trattamento che ha una base giuridica diversa dal consenso, come risultante dal Registro dei trattamenti.

4.3.1. Scelta delle misure di protezione

Ove non sia stata eseguita una DPIA, la scelta della tipologia di protezione dei dati di cui al punto b) compete al Responsabile interno del trattamento, sentito il DPO.

Il DPO deve sempre essere consultato ove la funzione ricevente richieda la trasmissione dei dati con applicazione di diversi sistemi di protezione.

4.3.2. Anonimizzazione e Pseudonimizzazione

Le modalità tecniche di anonimizzazione e pseudoanonimizzazione verranno valutate ad opera del Responsabile interno congiuntamente al DPO e alla Funzione Sistemi Informativi dell'Ospedale.

4.4 POLITICHE GENERALI RELATIVE ALLA COMUNICAZIONE DI DATI PERSONALI

La trasmissione di dati personali a terzi può avvenire:

a) ove l'interessato abbia prestato il proprio consenso al trasferimento;

b) ove sia necessario per adempiere ad un obbligo di legge ovvero la comunicazione dei dati risponda ad un rilevante interesse pubblico;

c) ove vi sia legittimo interesse della Fondazione prevalente rispetto a quello dell'interessato, ivi inclusi quelli:

(i) della tutela del patrimonio, mate riale e immateriale, della Fondazione;

(ii) della necessità di difesa della Fondazione e del personale che opera alle sue dipendenze ovvero in base ad altra tipologia di contratto;

d) ove vi sia un ordine dell'Autorità Giudiziaria competente.

Rientrano nelle ipotesi contemplate alla lettera b):

1) le comunicazioni di dati ad autorità pubbliche competenti nel settore del diritto del lavoro e della protezione sociale, comprese le pensioni, per finalità di sicurezza sanitaria, controllo e allerta, prevenzione e controllo di malattie trasmissibili e altre minacce gravi alla salute;

2) le comunicazioni fatte in ragione dell'inclusione della Fondazione nel novero delle strutture qualificate come ONLUS e comunque del Terzo Settore, secondo le normative italiane vigenti, per quanto applicabili;

3) per esigenze informative e richieste di comunicazioni fatte a soggetti pubblici e privati, compresa l'autorità giudiziaria, a fronte della necessità di accertare, esercitare o difendere un diritto sia in sede giudiziale, amministrativa o stragiudiziale, ivi incluso quello relativo ai rapporti con le assicurazioni per la responsabilità civile stipulate dalla Fondazione;

La trasmissione di dati è sempre fatta in maniera non eccedente le prescrizioni stabilite dalle norme vincolanti che le dispongono e, ove ciò non contrasti con le stesse o con le finalità da esse perseguite, previa anonimizzazione dei dati.

Le comunicazioni eseguite nel perseguimento del legittimo interesse della Fondazione o di suoi dipendenti sono fatte in maniera non eccedente le necessità che le hanno determinate e sono precedute dall'adozione di misure di protezione di anonimizzazione e pseudonimizzazione.

5 DIRITTI DELL'INTERESSATO

Gli interessati, rispetto ai dati personali che li riguardano, hanno diritto di:

a) ottenere la conferma che sia in corso un trattamento di dati personali che li riguardano e, in tal caso, di ottenere l'accesso ai dati personali e informazioni sui trattamenti;

b) ottenere la rettifica dei dati personali inesatti che li riguardano ovvero se pertinente rispetto al trattamento l'integrazione dei dati personali incompleti;

c) ottenere la limitazione dei trattamenti;

d) ricevere copia elettronica dei dati personali che li riguardano e da loro forniti;

e) opporsi in qualsiasi momento, per motivi connessi alla loro situazione particolare, al trattamento automatizzato di dati.

Il Responsabile interno del trattamento deve renderne immediata comunicazione al DPO per l'espressione di parere al riguardo.

Ove la richiesta sia ricevuta direttamente dal DPO questi informa il Responsabile interno del trattamento facendo pervenire contestualmente la sua opinione al riguardo.

Il DPO al fine di consentire un più celere riscontro agli interessati sulla base della casistica riscontrata ovvero di mutamenti normativi o giurisprudenziali rilascia delle linee di indirizzo generali sull'esercizio dei diritti degli interessati e le aggiorna annualmente.

Il Responsabile interno del trattamento comunica a ciascuno dei destinatari, ivi inclusi i contitolari, cui sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate su richiesta dell'interessato. Sentito il DPO, detta comunicazione può essere omessa quando ciò si riveli impossibile o implichi uno sforzo sproporzionato.

6 VIOLAZIONE DEI DATI

Eventuali violazioni di dati personali devo no essere tempestivamente comunicate al Titolare e al DPO (entro 24 ore dall'evento).

La comunicazione deve indicare:

a) la natura della violazione dei dati personali e le possibili cause;

b) le categorie e il numero approssimativo di interessati e/o delle registrazioni dei dati personali in questione;

c) le probabili conseguenze della violazione dei dati personali;

d) le misure adottate o di cui si propone l'adozione per porre rimedio alla viola- zione dei dati personali e per attenuarne i possibili effetti negativi.

7 FORMAZIONE INIZIALE E CONTINUA

Il Responsabile interno provvede a rendere edotti e idoneamente formato e aggiornato il personale Autorizzato al trattamento dei dati al fine di renderlo consapevole:

- dei rischi che incombono sui dati;
- delle misure per prevenire eventi dannosi;
- della disciplina sulla protezione dei dati più rilevanti in rapporto alle rispettive attività;
- delle responsabilità che ne derivano;
- delle modalità per aggiornarsi sulle misure minime adottate da OPBG.

Tale formazione avviene con frequenza e in occasione di cambiamenti di mansioni e dell'introduzione di nuovi e significativi strumenti rilevanti per il trattamento dei dati.

Fondazione Bambino Gesu'
Onlus
Il Presidente