Fondazione I.R.C.C.S.
Istituto Neurologico Carlo Besta

Sistema Socio Sanitario
Regione Lombardia

# CONSIGLIO DI AMMINISTRAZIONE

DELIBERAZIONE N. **V/** 131 **-2022** Seduta n. 46 del 21 dicembre 2022

Presiede il Presidente Andrea Gambini

Consiglieri Paolo Lazzati
Sonia Madonna
Monica Maggioni
Marta Marsilio
Francesca Zanconato

| | |
|---|---|
| Oggetto: | Regolamento della Fondazione per l'attuazione del Regolamento UE/2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali: modifiche e integrazioni. |

Il Direttore Generale
Angelo Cordone

Il Direttore Scientifico
Giuseppe Lauria Pinter

Il Direttore Amministrativo
Angela Pezzolla

Il Direttore Sanitario
Stefano Schieppati

Il Responsabile del procedimento: UOC Affari generali e Legali - Enzo Quadri

Visto: Il Direttore del Dipartimento Amministrativo – Mauro Lorenzo Rossi

L'atto si compone di n. **28** pagine, di cui n. 23 pagine di allegati, parte integrante

## IL CONSIGLIO DI AMMINISTRAZIONE

VISTI:

- la Legge Regionale 30 dicembre 2009 n. 33 e s.m.i. recante il *"Testo unico delle Leggi Regionali in materia di sanità"*;
- il D.lgs. 16 ottobre 2003 n. 288 *"Riordino della disciplina degli Istituti di Ricovero e Cura a Carattere Scientifico a norma dell'articolo 42, comma 1 della Legge 16 gennaio 2003 n. 3"*, recante disposizioni sugli Statuti degli Istituti trasformati in Fondazioni;
- il Decreto del Ministero della Salute del 28 aprile 2006 con cui è stata disposta la trasformazione dell'IRCCS Istituto Neurologico "Carlo Besta" in Fondazione IRCCS Istituto Neurologico "Carlo Besta";

RICHIAMATO lo Statuto della Fondazione, approvato dal Consiglio di Amministrazione con deliberazione 6 febbraio 2012, n. III/9;

VISTO il Regolamento Generale sulla Protezione dei dati personali - Regolamento UE 2016/679 - di seguito indicato "GDPR" - in vigore a far tempo dal 25 maggio 2018 in tutti i Paesi dell'Unione Europea, con il quale la Commissione Europea ha inteso rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno che all'esterno dei confini dell'Unione Europea;

RICHIAMATE le principali disposizioni introdotte dal GDPR di seguito sintetizzate:

- responsabilità diretta del titolare del trattamento in merito al compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;
- istituzione della figura obbligatoria del Responsabile della Protezione dei Dati (RPD/DPO), incaricato di assicurare una gestione corretta dei dati personali negli Enti;
- introduzione del *"Registro delle attività del trattamento"*, che tenuto a cura del Titolare del Trattamento (art. 30 comma 1 del GDPR) e del *"Registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare"*, tenuto a cura di ogni Responsabile del Trattamento (art. 30 comma 2 del GDPR), registri nei quali devono essere descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'Ente e devono contenere specifici dati indicati dal GDPR;
- obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati (c.d. D.P.I.A.), quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

DATO ATTO che l'adozione delle disposizioni contenute nel GDPR ha inciso sull'organizzazione interna di Imprese e P.A., in quanto ha richiesto la ricognizione e la valutazione delle misure di sicurezza normative, organizzative e tecnologiche, già adottate a tutela della privacy;

RICORDATO che con Deliberazione del C.d.A. n. IV/212, del 23 luglio 2018 è stato approvato il *"Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"*, in cui sono stati definiti l'ambito di applicazione, le responsabilità, i termini e le modalità di attuazione del GDPR;

DATO ATTO che a seguito dell'entrata in vigore del D.Lgs. 10 agosto 2018, n. 101, contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del Regolamento Europeo 2016/679 (GDPR), con Deliberazione del C.d.A. n. IV/240, del 12 novembre 2018, era stato approvato il nuovo testo del "*Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*", che aveva annullato e sostituito il precedente adottato con Deliberazione del C.d.A. n. IV/212, del 23 luglio 2018, emendato ed aggiornato alle novità normative introdotte dal suddetto D.Lgs. 10 agosto 2018, n. 101;

RAVVISATA la necessità di aggiornare il succitato Regolamento alla luce di nuove disposizioni normative in materia di trattamento dei dati personali, alle attuali disposizioni organizzative interne nonché alle modalità di gestione dei dati relativi ai pazienti nell'ambito dell'assistenza e in particolare nel settore della ricerca scientifica;

VISTO il testo emendato ed aggiornato del citato Regolamento Aziendale secondo quanto sopra descritto, predisposto dalla SC Affari Generali e Legali;

DATO ATTO che il presente provvedimento non comporta oneri aggiuntivi a carico del Bilancio d'esercizio della Fondazione;

DATO ATTO che il presente provvedimento è adottato dal Consiglio di Amministrazione ai sensi dell'art. 13 dello Statuto, su proposta del Presidente;

RITENUTO pertanto di approvare il testo aggiornato del "*Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" allegato al presente provvedimento quale parte integrante e sostanziale, che annulla e sostituisce il precedente adottato con Deliberazione del Consiglio di Amministrazione IV/240, del 12 novembre 2018;

ACQUISITO il parere di regolarità tecnica e di legittimità da parte del Direttore della S.C. Affari Generali e Legali;

Ad unanimità di voti espressi nelle forme di legge,

DELIBERA

di prendere atto di quanto in premessa descritto e conseguentemente:

1) di approvare il testo aggiornato del "*Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" allegato al presente provvedimento quale parte integrante e sostanziale, che annulla e sostituisce il precedente adottato con Deliberazione del Consiglio di Amministrazione IV/240, del 12 novembre 2018;

2) di dare atto che il citato Regolamento entrerà in vigore dalla data di pubblicazione del presente provvedimento nell'Albo pretorio on line della Fondazione;

3) di pubblicare il Regolamento nella sezione *"Amministrazione Trasparente"* del sito istituzionale della Fondazione;

4) di dare atto che il presente provvedimento non è soggetto a controllo ai sensi dell'art 17 comma 6 della Legge Regionale 33/2009 e ss.mm.ii.

IL PRESIDENTE
(Andrea Gambini)

In qualità di sostituto del Presidente
Ai sensi dell'art. 15 comma 5 dello Statuto
Avv. Sonia Madonna

Allegato:
- Regolamento della Fondazione per l'attuazione del Regolamento UE/2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Responsabile del procedimento:
Il Direttore della S.C. Affari Generali e Legali – Avv. Enzo Quadri

Addetto all'istruttoria: Alessandra Marasca

Proposta di Deliberazione CDA della **SC Affari Generali e Legali**

**OGGETTO:** Regolamento della Fondazione per l'attuazione del Regolamento UE/2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali: modifiche e integrazioni.

## ATTESTAZIONE DI REGOLARITA' TECNICA

Il Responsabile del Procedimento attesta la regolarità tecnica e la legittimità della proposta di delibera sopra citata.

IL DIRETTORE
(Avv. Enzo Quadri)

Milano, 14/12/2022

## ATTESTAZIONE DI REGOLARITA' CONTABILE

Il Responsabile della SC Bilancio e Programmazione Finanziaria attesta che la delibera in oggetto non comporta alcun onere a carico della Fondazione.

SC BILANCIOE PROGRAMMAZIONE FINANZIARIA

Il Direttore (Dott.ssa Angela Regina Volpe)

Milano, 16.12.2022

Fondazione I.R.C.C.S.
Istituto Neurologico Carlo Besta

Sistema Socio Sanitario
Regione Lombardia

ALLEGATO ALLA DELIBERA DEL CDA N. 131/22

# Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

**Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

Premesse ..... 3
Art. 1 Oggetto ..... 4
Art. 2 Definizioni ..... 4
Art. 3 Trattamento dei dati da parte di un'Amministrazione Pubblica ..... 6
Art. 4 Presupposti di liceità del trattamento ..... 6
Art. 5 Principi applicabili al trattamento dei dati personali ..... 7
Art. 6 Titolare del trattamento ..... 8
Art. 7 Organizzazione interna del Titolare del trattamento - Responsabili Privacy di Unità ..... 9
Art. 8 Organizzazione interna del Titolare del trattamento – Autorizzati ..... 10
Art. 9 Responsabili esterni del trattamento ..... 10
Art. 10 Responsabile della protezione dati – Data Protection Officer (DPO) ..... 11
Art. 11 Sicurezza del trattamento ..... 13
Art. 12 Informazioni per la raccolta dei dati ..... 14
Art. 13 Rilascio delle Informative in caso di emergenze e tutela della salute e dell'incolumità fisica ..... 15
Art. 14 Registro delle attività di trattamento ..... 15
Art. 15 Registro delle categorie di attività trattate ..... 16
Art. 16 Valutazioni d'impatto sulla protezione dei dati (DPIA) ..... 16
Art. 17 Violazione dei dati personali ..... 19
Art. 18 Il diritto di accesso e il diritto alla riservatezza ..... 21
Art. 19 Cartelle cliniche elettroniche ..... 21
Art. 20 Misure organizzative per la tutela della riservatezza ..... 21
Art. 21 Ricerca medica, biomedica ed epidemiologica ..... 22
Art. 22 Rinvio ..... 23

**Premesse**

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale dell'individuo, sancito dall'Articolo 8 della Carta dei diritti fondamentali dell'Unione Europea e dall'Articolo 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE).

È indispensabile garantire un livello elevato di protezione dei dati personali coerente con i rischi che le attività di trattamento effettuate comportano, rispetto ai diritti e alle libertà fondamentali dei soggetti interessati. La normativa vigente sulla quale si fonda il Regolamento sulla protezione dei dati della Fondazione "Carlo Besta" riguarda:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (Regolamento Generale sulla Protezione dei Dati "GDPR");
- Decreto Legislativo n. 196 del 30 giugno 2003 recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal Decreto Legislativo n. 101 del 10 agosto 2018 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 (regolamento generale sulla protezione dei dati)";
- D.L. 08/10/2021 n° 139 convertito con modificazioni dalla L. 03/12/2021 n° 205 - Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali;
- Linee guida emanate dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'articolo 14-bis, comma 2, lettera a), del Decreto Legislativo n. 82 del 7 marzo 2005 "Codice dell'amministrazione digitale", per come aggiornato dal Decreto Legislativo n. 217 del 13 dicembre 2017;
- Provvedimenti, linee guida e pareri emanati dall'Autorità Garante per la protezione dei dati personali;
- Linee guida adottate dal Comitato europeo per la protezione dei dati ("European Data Protection Board", EDPB), nonché dal precedente Gruppo di lavoro "Articolo 29" (WP29);
- Procedure, istruzioni operative nonché atti organizzativi, delibere e determine ed ogni altro documento interno all'Organizzazione del titolare del trattamento che risulti funzionale al raggiungimento delle finalità della presente Regolamento.

**Art. 1 Oggetto**

Il presente Regolamento ha lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la Fondazione. Il Besta adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

**Art. 2 Definizioni**

1) «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;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «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;

7) «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di

dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «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;

14) «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;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE 2016/679;

17) «Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente; oppure
- influenzati in modo sostanziale dal trattamento;
- un reclamo è stato proposto a tale autorità di controllo.

**Art. 3 Trattamento dei dati da parte di un'Amministrazione Pubblica**

Ai sensi dell'art. 9 del D. L. 08/10/2021 n° 139 convertito in legge con modificazioni dalla L. 3 dicembre 2021, n. 205, il trattamento dei dati personali da parte di un'Amministrazione Pubblica di cui all'art. 1, comma 2 del D. Lgs. 30/03/2001, n° 165, è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti. La finalità del trattamento, se non prevista da una norma di legge o di regolamento, è indicata dall'Amministrazione, assicurando adeguata pubblicità all'identità del titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare il trattamento corretto e trasparente con riguardo ai soggetti interessati, ai loro diritti di ottenere conferma e comunicazione di un trattamento dei dati personali che li riguardano.

Laddove fosse necessario procedere con un trattamento non previsto da una norma di legge o di regolamento, è obbligatorio fare una richiesta circostanziata all'Ufficio Protezione dei dati (dpo@istituto-besta.it) secondo una procedura appositamente predisposta dal Titolare del trattamento nel rispetto dell'art. 5 del Regolamento UE 2016/679. Eventuali procedure/trattamenti implementati senza le autorizzazioni dell'Ufficio Protezione dei dati sono da considerarsi illegittimi e le relative conseguenze saranno imputabili ai soggetti che le hanno poste in essere e che ne risponderanno per gli adempimenti di conseguenza.

**Art. 4 Presupposti di liceità del trattamento**

1. I trattamenti sono compiuti dalle Aziende del Sistema Sanitario Regionale sulla base dei seguenti presupposti di liceità:

a) prestazione del consenso da parte dell'interessato;

b) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;

c) adempimento di un obbligo legale al quale è soggetta la Fondazione;

d) esecuzione di un contratto con soggetti interessati;

e) salvaguardia di interessi vitali dell'interessato o della collettività.

**Art. 5 Principi applicabili al trattamento dei dati personali**

Ogni trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali. I dati personali devono essere trattati in modo lecito e secondo correttezza e trasparenza nei confronti dell'interessato, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati. In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli Autorizzati al trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Il trattamento dei dati personali è effettuato dall'Istituto, in quanto soggetto pubblico, per lo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico e per l'espletamento delle funzioni istituzionali assegnate e previste dalle normative vigenti.

I trattamenti sono finalizzati all'erogazione delle prestazioni sanitarie nonché agli adempimenti amministrativi e contabili, di organizzazione e di controllo, con particolare riguardo alle attività di:

a) erogazione di prestazioni sanitarie, sia istituzionali che in libera professione (comprensive di tutte le attività di supporto), erogate in regime di ricovero, ordinario o diurno, di assistenza specialistica ambulatoriale, di Day Service o altre modalità, volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
b) esercizio delle funzioni amministrative di competenza dell'Istituto:
    1. gestione del personale dipendente, comprese le procedure di assunzione;
    2. gestione dei soggetti che intrattengono rapporti giuridici con l'Istituto, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno della Fondazione stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i consulenti, i tirocinanti, i volontari;
    3. gestione dei rapporti con i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
    4. gestione dei rapporti con i soggetti accreditati o convenzionati;
    5. gestione del contenzioso instaurato nei confronti dell'Istituto, dei rapporti con i legali e consulenti di parte;
    6. rapporti con l'Autorità Giudiziaria e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti;

Sono altresì effettuati i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti: l'adempimento di un obbligo legale al quale è soggetta la Fondazione; per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

**Art. 6 Titolare del trattamento**

Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare") è la Fondazione IRCCS Istituto Neurologico "Carlo Besta" nella figura del Direttore Generale.

Il titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: 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 per 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, salvo le limitazioni previste dagli artt. 17 par. 3 lett. C), 23 e 89 del Reg. UE 2016/679 e secondo le modalità di integrazione per la rettifica dei dati ai sensi dell'art. 110 par. 2 del D. Lgs. 196/2003, 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 adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, i titolari devono effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 16.

Il titolare, inoltre, provvede a:

a) designare i Responsabili interni del trattamento nelle persone del Direttore Scientifico, Direttore Amministrativo e del Direttore Sanitario, nonché i Responsabili Privacy di Unità (RPU) di cui all'articolo 4, gli autorizzati -di cui all'art. 5 che operano nelle singole strutture in cui si articola l'organizzazione aziendale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati (RPD) – Data Protection Officer (DPO);

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, relativamente alle banche dati gestite da soggetti esterni alla Fondazione in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Azienda da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

La Fondazione favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili esterni del trattamento.

**Art. 7 Organizzazione interna del Titolare del trattamento - Responsabili Privacy di Unità**
**Il Responsabile Privacy di Unità** è responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di competenza e deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

Il Titolare del trattamento designaquali **Responsabili Privacy di Unità** , per le rispettive aree di competenza, le seguenti figure :

- Direttori di Dipartimento;

- Direttori di Struttura Complessa;

- Responsabili di Strutture Semplici Dipartimentali;

- Responsabili di Strutture Semplici.

Nella lettera di designazione, il Titolare del trattamento conferisce ai suddetti RPU il compito di attuare le politiche e le procedure organizzative della Fondazione in materia di protezione dei dati personali nell'ambito della rispettiva struttura di afferenza, conformemente alle disposizioni normative vigenti.

**Art. 8 Organizzazione interna del Titolare del trattamento – Autorizzati**

Il Titolare del trattamento, per il tramite dei Responsabili Privacy di Unità, individua i soggetti **Autorizzati al trattamento**, ai sensi dell'art. 29, del GDPR "216/679, intesi come persone fisiche autorizzate a compiere operazioni di trattamento. I soggetti individuati come autorizzati al trattamento sono designati con nota di incarico a firma dell'RPU.

**Art. 9 Responsabili esterni del trattamento**

Il Titolare può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di **Responsabili esterni** del trattamento (ai sensi dell'art. 28 del GDPR), forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

Gli atti che disciplinano il rapporto tra il titolare ed i Responsabili esterni del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile esterno del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed i Responsabili esterni; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile esterno attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile esterno risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

Il Responsabile esterno del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il Responsabile esterno del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;

- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;

- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

- alla designazione del Responsabile per la Protezione dei Dati (RPD), se previsto dalla legge;

- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;

- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

**Art. 10 Responsabile della protezione dati – Data Protection Officer (DPO)**

Il Responsabile della protezione dei dati – Data Protection Officer (in seguito indicato con "DPO") è individuato in un soggetto esterno / società scelta tramite procedura ad evidenza pubblica.

Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione. A

tali fini il nominativo del DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

Il Titolare ed il Responsabile del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;

- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il DPO:

-procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

- definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio della Fondazione.

La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili (in relazione alle dimensioni organizzative della Fondazione):

- il Responsabile per la prevenzione della corruzione e per la trasparenza;

- i Responsabili interni e i sub responsabili del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare ed i Responsabili interni e i sub responsabili del trattamento forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al DPO:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e degli altri organi di natura amministrativa e politica, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio e di Piano della performance;

- tempo sufficiente per l'espletamento dei compiti affidati al DPO;

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno della Fondazione;

- accesso garantito ai settori funzionali della Fondazione così da fornirgli supporto, informazioni e input essenziali.

Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dai Responsabili Interni del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare - o suo delegato - od ai Responsabili interni del trattamento. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed ai Responsabili interni del trattamento.

**Art. 11 Sicurezza del trattamento**

Il Titolare e i Responsabili esterni del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento possono ricomprendere, se del caso: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Il titolare e ciascun Responsabile esterno del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, e del Responsabile della protezione dati – Data Protection Officer sono pubblicati sul sito istituzionale della Fondazione, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

**Art. 12 Informazioni per la raccolta dei dati**

La Fondazione Besta, quale titolare del trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati quali l'identità ed i dati di contatto del titolare del trattamento, i dati di contatto del responsabile della protezione dei dati, le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento, i legittimi interessi perseguiti dal titolare del trattamento o dai terzi, gli eventuali destinatari dei dati personali.

Nel momento in cui i dati personali sono ottenuti, il Titolare fornisce all'interessato ulteriori informazioni per garantire un trattamento corretto e trasparente quali:

a) l'identità ed i dati di contatto del titolare del trattamento;
b) i dati di contatto del responsabile della protezione dei dati;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
f) il periodo di conservazione dei dati personali, oppure se non è possibile, i criteri utilizzati per determinare tale periodo;

g) l'esistenza del diritto dell'interessato di chiedere al titolare l'accesso ai dati personali e la rettifica o la cancellazione degli stessi, ove possibile, o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
h) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
i) il diritto di proporre reclamo ad un'autorità di controllo;
j) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
k) esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora l'Istituto intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Qualora i dati non siano stati ottenuti presso l'interessato, l'Azienda fornisce all'interessato le anche le informazioni relative alla fonte dalla quale ha tratto i suoi dati.

**Art. 13 Rilascio delle Informative in caso di emergenze e tutela della salute e dell'incolumità fisica**

Le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679 possono essere rese senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica.
Tali informazioni possono altresì essere rese senza ritardo, successivamente alla prestazione, in caso di:
a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;
b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.
Le informazioni di cui al presente articolo possono essere rese senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.
Dopo il raggiungimento della maggiore età le informazioni sono fornite all'interessato nel caso in cui non siano state fornite in precedenza.

**Art. 14 Registro delle attività di trattamento**

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto della Fondazione, del Direttore Generale, eventualmente del Contitolare del trattamento, e del DPO;

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, come da precedente art.6.

Il Registro è tenuto dal Titolare presso gli uffici della struttura organizzativa aziendale in forma telematica; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative della Fondazione.

**Art. 15 Registro delle categorie di attività trattate**

Il Registro delle categorie di attività trattate dalla Fondazione in qualità di responsabile esterno di un Titolare del trattamento terzo conterrà 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 di ogni titolare del trattamento;

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

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

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

**Art. 16 Valutazioni d'impatto sulla protezione dei dati (DPIA)**

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto del Provvedimento del Garante Privacy 11 ottobre 2018 n° 467 relativo all'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati dal ai sensi dell'art. 35, pp. 4-6, del Regolamento (UE) n. 2016/679.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti della Fondazione, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere

che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno alla Fondazione. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;

- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un DPO e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una

descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base: delle finalità specifiche, esplicite e legittime; della liceità del trattamento; dei dati adeguati, pertinenti e limitati a quanto necessario; del periodo limitato di conservazione; delle informazioni fornite agli interessati; del diritto di accesso e portabilità dei dati; del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento; dei rapporti con i responsabili del trattamento; delle garanzie per i trasferimenti internazionali di dati; consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

**Art. 17 Violazione dei dati personali**

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla Fondazione.

Il titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. I Responsabili esterni del trattamento

sono obbligati ad informare il titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;

- perdita del controllo dei dati personali;

- limitazione dei diritti, discriminazione;

- furto o usurpazione d'identità;

- perdite finanziarie, danno economico o sociale;

- decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione;

- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intendono adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

**Art. 18 Il diritto di accesso e il diritto alla riservatezza**

La Fondazione, in osservanza delle disposizioni vigenti in materia di riservatezza e trasparenza, valuta, anche con riguardo ad altre regolamentazioni specifiche, caso per caso, la possibilità da parte di terzi di accedere a documenti contenenti dati personali e particolari. L'accesso ai dati idonei a rivelare lo stato di salute o la vita sessuale o l'orientamento sessuale di un terzo (art. 60 Codice Privacy) è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango almeno pari al diritto alla riservatezza, ovvero consiste in un diritto della personalità o altro diritto o libertà fondamentale ed inviolabile, quale ad esempio il diritto alla difesa, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso. Fatto salvo quanto sopra, I presupposti, le modalità, i limiti per il diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla Legge 7/8/1990, n. 241 ed s.m.i. e dalle altre disposizioni di legge in materia. I presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal Decreto Lgs 14 marzo 2013, n. 33, come modificato dal D. Lgs n.97/2016 e s.m.i.

**Art. 19 Cartelle cliniche elettroniche**

La Fondazione ha avviato il procedimento per l'attivazione della Cartella Clinica Elettronica, strumento di lavoro che permette attraverso il diario giornaliero, la sistematica raccolta cronologica, logica e obiettiva delle informazioni sul paziente continuamente aggiornate, necessarie a formulare diagnosi più efficienti ed efficaci e alla progettazione del piano assistenziale definito per obiettivi da raggiungere.

Secondo quanto disposto dal Codice della Privacy 196/2003 come modificato dal D.Lgs. 101/2018, eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

**Art. 20 Misure organizzative per la tutela della riservatezza**

Presso tutte le Strutture della Fondazione Carlo Besta sono adottate procedure atte a garantire la riservatezza degli utenti quali:

- adozione di distanze di cortesia presso gli sportelli;

- divieto di esporre nei reparti o in altri locali aperti al pubblico liste di pazienti in attesa di intervento;
- divieto di chiamare per nome i pazienti in attesa del proprio turno;
- riservatezza nei colloqui con pazienti o familiari evitando di fornire notizie particolari in situazioni di promiscuità o in presenza di personale estraneo o non autorizzato;
- uso nei reparti di terapia intensiva di paraventi o simili al fine di limitare la visibilità del malato ai soli familiari o conoscenti;
- divieto di pubblicare dati personali di pazienti (nomi, foto, ecc.) sulle pagine di social network;
- divieto di effettuare riprese audiovideo con attrezzature specifiche, telefoni cellulari, tablet o altri strumenti tecnologici nei reparti, presso gli ambulatori, le sale d'attesa, il pronto soccorso, palestre, aree comuni ed in ogni altro luogo dove ci sono pazienti. Qualunque eccezione a queste disposizioni deve essere autorizzata dal personale responsabile.

**Art. 21 Ricerca medica, biomedica ed epidemiologica**

Quando il trattamento è effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica ovvero a fini statistici, è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità al Regolamento UE. Queste garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati, che possono includere la pseudonimizzazione.

Se i dati personali sono trattati a fini di ricerca scientifica o a fini statistici, il Codice della Privacy può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui sopra, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e queste deroghe sono necessarie al conseguimento di dette finalità.

Secondo quanto dispone il Codice della Privacy 196/2003 come modificato dal D.Lgs 101/2018, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente Comitato Etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

A norma dell'art. 110 bis del Codice della Privacy novellato, non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

**Art. 22 Rinvio**

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.