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

Sistema Socio Sanitario
Regione Lombardia

CONSIGLIO DI AMMINISTRAZIONE

DELIBERAZIONE N. **IV/** 240 Seduta n. 35 del 12 Novembre 2018

Presiede il Presidente Alberto Guglielmo

Consiglieri
Andrea Casini
Irvano Loatelli
Adriano Paroli
Francesco Bevere
Agostino Migone De Amicis
Paolo Lazzati

Con l'assistenza del Segretario: Paolo Tafuro

Su proposta : Direttore Generale Germano Pellegata

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

Il Direttore Scientifico
Fabrizio Tagliavini

Il Direttore Amministrativo
Maurizia Ficarelli

Il Direttore Sanitario
Angelo Cordone

Il Responsabile del procedimento: Il Direttore U.O.C. Affari Generali e Legali - Sandra Bazzoni

Visto: Il Direttore del Dipartimento Amministrativo – Marco Losi

L'atto si compone di n. **20** pagine, di cui n. **16** pagine di allegati, parte integrante

IL CONSIGLIO DI AMMINISTRAZIONE

RICHIAMATO il D.lgs. n. 502/1992 e successive modifiche ed integrazioni;

VISTA la Legge Regionale 30 Dicembre 2009 n. 33 "Testo unico delle Leggi Regionali in materia di sanità", come modificata e integrata dalla Legge Regionale n. 23 dell'11 Agosto 2015;

RICHIAMATO lo Statuto della Fondazione, approvato dal Consiglio di Amministrazione con deliberazione 6 Febbraio 2012 n. III/9, su cui la Regione Lombardia ha espresso il proprio parere di congruità con deliberazione della Giunta Regionale 7 Marzo 2012 n. 3080;

PREMESSO che a far tempo dal 25 Maggio 2018 è entrato in vigore in tutti i Paesi dell'Unione Europea il Regolamento Generale sulla Protezione dei dati personali (Regolamento UE 679/2016 - di seguito indicato "GDPR") 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;

DATO ATTO che le principali novità introdotte dall'GDPR possono essere così 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 dovrà essere tenuto a cura del Titolare del Trattamento (art. 30 comma 1 del GDPR) e il *"Registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare"*, che dovrà essere tenuto a cura di ogni Responsabile del Trattamento (art. 30 comma 2 del GDPR), registri nei quali dovranno essere descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'Ente e dovranno contenere specifici dati indicati dal GDPR;
- obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati, 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;

RICHIAMATA la Deliberazione del Consiglio di Amministrazione n. 212 del 23 Luglio 2018 con la quale è stato disposto di approvare il *"Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al*

trattamento dei dati personali", con il quale sono stati definiti l'ambito di applicazione, le responsabilità, i termini e le modalità di attuazione del GDPR;

PRESO ATTO che il 4 settembre 2018 è stato pubblicato nella Gazzetta Ufficiale n. 205 il decreto legislativo 101 del 10 agosto 2018 contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del Regolamento Europeo 2016/679 (GDPR) 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);

PRECISATO che la funzione del decreto legislativo n. 101/2018 è quella di armonizzare le norme enunciate dal legislatore nazionale nel Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) con quelle introdotte dal Regolamento Europeo 2016/679 entrato in vigore il 25 maggio 2018;

RITENUTO pertanto opportuno adeguare i contenuti del *"Regolamento Aziendale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"* alle disposizioni contenute nel sopra citato decreto legislativo n. 101/2018 e contestualmente riformulare gli articoli 2 *("Titolare del trattamento")* e 4 *("Organizzazione interna del Titolare del trattamento - Responsabile interno del trattamento")* adeguandoli alle peculiarità organizzative della Fondazione;

RITENUTO opportuno altresì ridefinire, in particolare l'articolo 4 *"Organizzazione interna del titolare del trattamento"*, prevedendo quale miglior assetto organizzativo la seguente articolazione:

- Titolare del trattamento: la Fondazione nella persona del Direttore Generale;
- Responsabili interni del trattamento: Direttore Scientifico, Direttore Amministrativo e Direttore Sanitario, che devono 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 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR;
- Sub-responsabili del trattamento:
  - Direttori di Dipartimento;
  - Direttori di Unità Operativa Complessa;
  - Responsabili di Strutture Dipartimentali;
  - Responsabili di Strutture Semplici;
  - Posizioni Organizzative;
  - Principal Investigator;

  che hanno l'obbligo di rispettare gli stessi obblighi che legano il Titolare del trattamento ed i Responsabili Interni:
- Incaricati del trattamento: persone fisiche autorizzate a compiere operazioni di trattamento;

VISTO il testo emendato ed aggiornato del citato Regolamento Aziendale secondo quanto sopra descritto, predisposto dagli uffici competenti;

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

ACQUISITO il parere di regolarità tecnica e di legittimità da parte del Direttore dell'U.O.C. Affari Generali e Legali;

VISTO l'art. 13 dello Statuto della Fondazione;

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 emendato ed aggiornato alle novità normative introdotte dal decreto legislativo n. 101/2018 nonché adeguato alle esigenze organizzative della Fondazione, 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 n. 212 del 23 Luglio 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 citato 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
(Alberto Guglielmo)

IL SEGRETARIO
(Paolo Tafuro)

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

Il Responsabile del procedimento:
Il Direttore dell'U.O.C. Affari Generali e Legali – Sandra Bazzoni

Addetto all'istruttoria: Angelo Carnelli

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

Sistema Socio Sanitario
Regione Lombardia

ALLEGATO ALLA DELIBERA DEL CDA N. 240/2018

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

ALLEGATO ALLA DELIBERA DEL CDA N. 240/2018

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

Art. 1 Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "GDPR", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nella Fondazione IRCCS Istituto Neurologico "Carlo Besta" e del D.Lgs. n. 196/2003 e s.i.m.

Art. 2 Titolare del trattamento

1. 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.

2. 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.

3. 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, 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.

4. 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.

5. 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. 9.

6. Il titolare, inoltre, provvede a:

a) designare i Responsabili interni del trattamento nelle persone del Direttore Scientifico, Direttore Amministrativo e del Direttore Sanitario, i sub responsabili di cui all'articolo 4, gli incaricati 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;

d) predisporre l'elenco dei Responsabili interni e dei sub responsabili del trattamento delle strutture in cui si articola l'organizzazione della Fondazione, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. 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.

8. 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. 3 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. 4 Organizzazione interna del Titolare del trattamento - Responsabili interni del trattamento e sub responsabili

1 **Il Responsabile Interno** 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.

2. Il Titolare del trattamento designa, mediante deliberazione del Direttore Generale, quali **Responsabili Interni** del trattamento per le rispettive aree di competenza:

- il Direttore Scientifico;

- il Direttore Amministrativo;

- il Direttore Sanitario.

Nella deliberazione/lettera di incarico sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in idoneo atto giuridico da stipularsi fra il Titolare e ciascun responsabile designato.

3. I Responsabili interni del trattamento hanno l'obbligo di **individuare** quali **Sub-Responsabili** del trattamento le seguenti figure:

- Direttori di Dipartimento;

- Direttori di Unità Operativa Complessa;

- Responsabili di Strutture Dipartimentali;

- Responsabili di Strutture Semplici;

- Posizioni Organizzative;

- Principal Invastigator.

I sub-responsabili saranno nominati dal Titolare del trattamento.

I sub-responsabili hanno l'obbligo di rispettare gli stessi obblighi che legano il Titolare del trattamento ed i Responsabili Interni; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile o del Sub-Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Art. 5 Organizzazione interna del Titolare del trattamento – Incaricati

Il Titolare del trattamento, i Responsabili interni del trattamento e i sub-responsabili di cui all'art. 4 individuano gli **Incaricati al trattamento** intesi come persone fisiche autorizzate a compiere operazioni di trattamento. I soggetti individuati come incaricati al trattamento sono designati con nota di incarico a firma del Direttore Generale, nel quale sono tassativamente disciplinati:

- l'elenco dei trattamenti, la durata dell'incarico, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- le modalità di esecuzione dell'incarico.

Tale disciplina può essere contenuta anche in idoneo atto giuridico da stipularsi fra il titolare e ciascun incaricato.

Art. 6 Responsabili esterni del trattamento

1. Il titolare può avvalersi, per il trattamento di dati, anche sensibili, 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.

2. 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.

3. 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.

4. 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.

5. 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 a ciò demandato dal Titolare;

- 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. 7 Responsabile della protezione dati – Data Protection Officer (DPO)

1. Il Responsabile della protezione dei dati – Data Protection Officer (in seguito indicato con "DPO") è individuato nella figura unica del Dott. Luigi Recupero, dipendente di ruolo di LTA S.r.l., 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.

2. 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.

3. 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:

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

b) 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.

4. 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.

5. 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.

6. 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.

7. 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. 8 Sicurezza del trattamento

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. I nominativi ed i dati di contatto del Titolare, dei Responsabili interni del trattamento 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.

7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art. 9 Registro delle attività di trattamento

1. 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.

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

Art. 10 Registro delle categorie di attività trattate

1. 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.

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

Art. 11 Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. 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.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, GDPR.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale 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.

10. 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. 12 Violazione dei dati personali

1. 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.

2. 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 48 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.

3. 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).

4. 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).

5. 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.

6. 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. 13 Rinvio

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