Regolamento

per la protezione dei dati personali delle persone fisiche

in osservanza del Regolamento UE 2016/679 (RGPD)

INDICE

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 "RGPD", Regolamento Generale per la Protezione dei Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati presso l'IRCCS Oncologico di Bari – Giovanni Paolo II (d'ora in avanti ITB).

Art. 2 – Titolare del trattamento

1. L'ITB, rappresentato ai fini previsti dal RGPD dal Direttore Generale pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Direttore Generale può delegare le relative funzioni ai Dirigenti e/o Direttori in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: 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 RGPD.

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 RGPD, 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 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non 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, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "VIP") ai sensi dell'art. 35, RGDP, 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, mediante atto individuale, in qualità di "Delegati al trattamento dei dati", tutti i Dirigenti delle singole Strutture (semplici, semplici dipartimentali e complesse) in cui si articola l'organizzazione dell'ITB, preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza**;

   b) **nominare il Responsabile della protezione dei dati**;

   c) **nominare quale Responsabile del trattamento (ex art. 28 del RGPD) i soggetti esterni pubblici o privati affidatari di attività e servizi per conto dell'ITB**, relativamente alle banche dati gestite da soggetti esterni all'ITB 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 Delegati al trattamento dei dati e dei Responsabili del trattamento (soggetti esterni), 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'ITB 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 RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. L'ITB" 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 RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 3 – Finalità del trattamento

I trattamenti sono compiuti dall'ITB per le seguenti finalità:

- tutela della salute e dell'incolumità fisica (prestazioni di prevenzione, diagnosi, cura e riabilitazione);
- attività legate alla fornitura di beni o servizi all'utente per la salvaguardia della salute (es. fornitura di ausili e protesi);
- adempimenti amministrativi, gestionali e contabili, correlati ai compiti istituzionali dell'ITB e/o connessi ad obblighi di legge;
- attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
- attività epidemiologica e statistica, ricerca scientifica, didattica e genetica nel rispetto dei limiti e delle condizioni dettate dalla disciplina in materia di protezione dei dati personali
- gestione di esposti/lamentele/contenziosi ed altri adempimenti previsti da specifiche norme di legge e/o regolamento.

Art. 4 – Delegati interni e Responsabili del trattamento

1. Il Regolamento Europeo (UE) 2016/679 dispone che il trattamento dei dati possa essere effettuato esclusivamente da parte di soggetti autorizzati.

2. A tale riguardo l'ITB ritiene opportuno, alla luce della sua complessità organizzativa e della numerosità dei soggetti che devono essere autorizzati a trattare i dati, conferire con apposita delega una funzione di coordinamento del trattamento dei dati personali a taluni collaboratori dotati dei requisiti di esperienza, capacità e affidabilità tali da fornire idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza.
3. Ciascun **Dirigente di di Area, S.C., S.S. e SSD, è nominato dal Direttore Generale quale "Delegato al trattamento dei dati" di tutte le banche dati esistenti nell'articolazione organizzativa di rispettiva competenza.** Il **"Delegato al trattamento dei dati"** deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. **Con riferimento alle misure tecnologiche e di sicurezza informatica, adeguate al rischio insito nel trattamento dei dati, ai sensi dell'art. 32 del RGPD, ciascun "Delegato interno per la protezione dei dati" è opportunamente supportato dall'Area Tecnica e Servizi Informatici dell'ITB;**
4. Ciascun "Delegato al trattamento dei dati" è tenuto a designare i soggetti autorizzati al trattamento dei dati, nell'Area di propria competenza, mediante atto individuale;
5. **Il Titolare può avvalersi, per il trattamento di dati personali e sensibili, di soggetti esterni pubblici o privati che, in qualità di Responsabili del trattamento, ai sensi dell'art. 28 del RGPD, forniscano adeguate garanzie,** 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.
6. **Gli atti** che **disciplinano il rapporto tra il Titolare ed il Responsabile (esterno) del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD;** tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
7. **E'** consentita **la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento** per specifiche attività di trattamento, nel rispetto degli

stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile 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.

8. **Il Responsabile 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.**
9. Il "Delegati al 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:
   - al supporto finalizzato all'aggiornamento del registro delle attività di trattamento svolte per conto del Titolare;
   - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti, **con il supporto dell'Area Sistemi Informatici dell'ITB** per quanto di competenza;
   - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
   - ad assistere il Titolare ed il Responsabile della protezione dei dati (RPD) nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "VIP") fornendo allo stesso ogni informazione di cui è in possesso;
   - ad informare il Titolare ed il Responsabile della protezione dei dati (RPD), senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione all'Autorità Garante per la protezione dei dati, 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. 5 – Responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è designato dal Titolare in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento UE 2016/679, che di seguito sono elencati:

   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 RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD 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 RGPD 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 "Delegati al trattamento dei dati";

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

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 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) (eventuale) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) 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 RPD.

2. Il Titolare ed il "Delegati al trattamento dei dati" assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD 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 RPD 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 RPD, è necessario motivare specificamente tale decisione;

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

3. Nello svolgimento dei compiti affidatigli il RPD 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 RPD:

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. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento;
5. Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Art. 6 – Gli Amministratori di Sistema

L' ITB, in qualità di Titolare del trattamento, individua i soggetti operanti sulla rete informatica, in qualità di Amministratori di Sistema, per ambito di operatività consentito. Nel caso di dipendenti dell'ITB autorizzati dal Titolare ad accedere alla rete informatica aziendale, ai computer e server con privilegi amministrativi, per fini di manutenzione ed assistenza, si procede con atto formale di nomina corredato di apposite istruzioni operative.

Nel caso di presenza di soggetti terzi (consulenti, ditte e società) autorizzati all'erogazione di servizi di assistenza sistemistica, di gestione della sicurezza informatica e monitoraggio della rete informatica, il Titolare del trattamento individua la persona giuridica in qualità di Responsabile del trattamento, ai sensi dell'art. 28 del RGPD, con la formalizzazione di un contratto tra le parti, al fine di specificare i compiti e le responsabilità di cui all'art. 4 del presente Regolamento.

Art. 7 – Informativa

L' ITB, in qualità di Titolare del trattamento, predispone le informative generali sul trattamento dei dati personali chiare e comprensibili per fornire all'interessato tutte le

informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Le informazioni da rendere all'utenza, ai sensi dell'artt. 13-14 del RGPD, riportano almeno quanto segue:

- l'identità e 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;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo ;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- 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;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Ulteriori trattamenti di dati personali, che potrebbero presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, sono effettuati, in conformità alle leggi e ai regolamenti, previa ulteriore nota informativa e, dove richiesto, previo rilascio del consenso dell'interessato, manifestato liberamente.

L'informativa viene resa agli interessati attraverso:

- la pubblicazione delle informazioni ex artt. 13-14 del RGPD sul sito internet istituzionale;

- mediante affissione di appositi cartelli nelle sale d'attesa e negli altri locali di affluenza del pubblico;
- mediante appositi moduli da consegnare agli interessati;
- mediante stampa o invio tramite email su richiesta dell'interessato.

Art. 8 – I diritti degli interessati

Gli interessati possono contattare il Responsabile della protezione dei dati dell'ITB per l'esercizio dei loro diritti. L'interessato (assistito/assistibile) ha il diritto di ottenere dall' ITB la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e in tal caso, ottenere l'accesso ai dati e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'ITB si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e

libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 9 – Il diritto di accesso e il diritto alla riservatezza

L' ITB, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta anche con riguardo ad altre regolamentazioni specifiche, caso per caso la possibilità degli interessati di accedere ai documenti. L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali 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 alla personalità o in un altro diritto o libertà fondamentale o inviolabile, quale ad esempio il diritto alla difesa. Ulteriori specifiche indicazioni agli operatori sono contenute negli altri regolamenti o istruzioni operative adottate dall' ITB.

Art. 10 – Liceità del trattamento e Consenso

I dati personali possono essere trattati soltanto:

- da parte del Titolare, dei Contitolari, dei Delegati al trattamento dei dati, dei soggetti autorizzati, dei Responsabili del trattamento dei dati personali e degli Amministratori di Sistema

Se previsto da Legge e se sono raccolti e registrati per scopi determinati, espliciti e legittimi quando:

a) l'interessato ha prestato il consenso esplicito al trattamento dei dati personali per una o più finalità specifiche;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni;
g) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali o conformemente al contratto con un professionista della sanità;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
Nel caso in cui il trattamento dei dati personali sia basato sul rilascio del preventivo consenso da parte dell'interessato (ad es. in caso di degenza, Dossier Sanitario, Refertazione online etc.), è compito dell'ITB dimostrare che questi abbia prestato il proprio consenso libero ed informato al trattamento dei dati personali.
Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre finalità o ulteriori specifici trattamenti di dati personali, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma facilmente accessibile e comprensibile.
Il Titolare assicura un'appropriata conservazione dei consensi espressi dagli interessati al fine di consentire un agevole esercizio dei diritti degli interessati.

Art. 11 – Sicurezza del trattamento

1. L' ITB e ciascun "Delegato al trattamento dei dati" mettono in atto misure tecniche ed organizzative adeguate, con il supporto dell' Area Tecnica e Servizi informatici, al fine di 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 ricomprendono: 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:
   - i sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; registrazione accessi etc..);
   - le 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 RGDP 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. L' ITB e ciascun "Delegati al trattamento dei dati" si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali di cui è titolare l'ITB.
6. I nominativi ed i dati di contatto del Titolare, dei "Delegati al trattamento dei dati", dei Responsabili del trattamento ex art. 28 del RGPD e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'ITB.

Art. 12 – Registro delle attività del trattamento

1. Il Titolare del trattamento, con il supporto del Responsabile della protezione dei dati e la collaborazione del personale tutto dell' ITB, predispone il Registro delle attività di trattamento recante almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Titolare del trattamento dei dati ed eventualmente del Contitolare del trattamento, e del Responsabile della protezione dei dati;
   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 del trattamento in formato digitale, con il supporto dell'Area Tecnica e Servizi informatici.
3. Il Titolare del trattamento può decidere di affidare al Responsabile della protezione dei dati (RPD) il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Art. 13 – Valutazione di impatto Privacy

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 (VIP – valutazione d'impatto privacy) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La VIP 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 VIP si tiene conto degli elenchi delle tipologie di trattamento soggetti a valutazione come previsti dal RGDP e come approvati dal Comitato Europeo per la protezione dei dati (EDPB) nella terza riunione plenaria.
3. La VIP 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, RGDP, 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, RGDP;

   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 dell' ITB, 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 VIP, 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 VIP.

4. Il Titolare garantisce l'effettuazione della VIP ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della VIP ad un altro soggetto, interno o Esterno all'organizzazione.

   Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la VIP; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della VIP. Il RPD monitora lo svolgimento della VIP.

   Il Responsabile del trattamento deve assistere il Titolare nella conduzione della VIP 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 VIP.

5. Il RPD può proporre lo svolgimento di una VIP, con il supporto dell'Area Tecnica e dei Servizi Informatici, 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 VIP in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La VIP 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, RGDP;

- 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 VIP. In questo caso si possono utilizzare i risultati della VIP 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 VIP all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una VIP per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP 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 VIP 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 RGPD, 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 VIP 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 VIP 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. 14 – 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 dall' ITB.

2. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Ciascun "Delegato al trattamento dei dati" informa il Titolare del trattamento, anche per il tramite del Responsabile della protezione dei dati, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare, con il supporto del Responsabile della protezione dei dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La notifica formale è effettuata dal Titolare, ove ritenuta necessaria, tramite posta elettronica certificata con l'invio del modello per la segnalazione predisposto dal Garante, all'indirizzo email databreach.pa@pec.gpdp.it.

3. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con

un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni :

a) la natura della violazione dei dati

b) i dati di contatto del Responsabile della protezione dei dati

c) le possibili conseguenze della violazione

d) le misure adottate o di cui si propone l'adozione per porvi rimedio

Non è richiesta la comunicazione all' interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.
5. Nel caso di violazione dei dati personali il Titolare del trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.
6. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale

significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

7. Il Titolare, con il supporto del Responsabile della protezione dei dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente il Garante e l'interessato, se del caso.
8. A seguito valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della protezione dei dati, adotta una le seguenti azioni:
   a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento;
   b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/679;
   c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai p.ti a) e b).

Pertanto, il Titolare del trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare al Garante che il *data-breach* non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

9. Ciascun "**Delegato** al trattamento dei dati" (Dirigente di Struttura), per ambito di competenza ed in generale tutto il personale aziendale, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati :
   - Direttore Generale
   - Responsabile della protezione dei dati
   - Responsabile Area Sistemi Informatici

   La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto interno, utilizzando il modello in allegato al presente Regolamento *(Modello segnalazione interna data-breach).* Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati:
   - Direttore Sanitario
   - Responsabile della protezione dei dati
   - Responsabile Area Sistemi Informatici
   - Responsabile della Struttura interessata dal *data-breach*

   Il Responsabile della protezione dei dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.

   Il Responsabile della protezione dei dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario.

   A conclusione della valutazione della violazione, il Responsabile della protezione dei dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti.

10. Il Titolare del trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità.

Il registro delle violazioni è custodito dal Responsabile della protezione dei dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/679.

11. Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del Regolamento UE 2016/679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.
Il Titolare del trattamento o il Responsabile del trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
La violazione delle disposizioni contenute nel Regolamento 2016/679 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro.

Art. 15 – Rinvio

Per quanto non espressamente previsto nel presente Regolamento si fa rinvio al Regolamento UE 679/2016 e successive regolamentazioni.
Il Titolare del trattamento si riserva di modificare e integrare il presente Regolamento, ove ritenuto necessario, anche alla luce di eventuali successive innovazioni normative o pronunciamenti dell'Autorità Garante per la protezione dei dati.

Art. 16 – Allegati

- modello per la segnalazione di violazioni dei dati *(c.d. data-breach)* ad uso interno
- modelli informative sul trattamento dei dati personali
- modello atto di nomina dei soggetti autorizzati al trattamento.