Azienda Sanitaria Locale della Provincia di Foggia

Attuazione del Regolamento UE
2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Regolamento interno per la protezione dei dati delle persone fisiche

INDICE

Art. 1 - Oggetto 2
Art. 2 – Titolare del trattamento 2
Art. 3 – Finalità del trattamento 4
Art. 4 – Delegati interni e Responsabili del trattamento 5
Art. 5 – Responsabile della protezione dei dati 9
Art. 6 – Gli Amministratori di Sistema 11
Art. 7 – Informativa e Consenso 12
Art. 8 – I diritti degli interessati 17
Art. 9 – Il diritto di accesso e il diritto alla riservatezza 18
Art. 10 – Liceità del trattamento 18
Art. 11 – Sicurezza del trattamento 19
Art. 12 – Registro delle attività del trattamento 21
Art. 13 – Valutazione di impatto sulla protezione dei dati 22
Art. 14 – Violazione dei dati personali 26
Art. 15 – Rinvio 31
Art. 16 – Allegati 31

Art. 1 - Oggetto

1. Il presente Regolamento è uno strumento di applicazione del vigente decreto legislativo 30 giugno 2003, n. 196 (il cosiddetto "Codice sulla privacy"), così come modificato dal decreto legislativo 10 agosto 2018 n. 101(Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016) e del Regolamento UE 2016/679, nell'ambito dell'organizzazione aziendale.
2. 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 presso l'Azienda Sanitaria Locale della Provincia di Foggia** (d'ora in avanti ASL di Foggia).

Art. 2 – Titolare del trattamento

1. L'ASL di Foggia, rappresentata dal Direttore Generale pro tempore ai fini del GDPR, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Titolare del trattamento, ai sensi dell'art. 2 quaterdecies del D.lgs. 196/03, così come modificato dal D.lgs. 101/18, può prevedere che specifici compiti e funzioni connessi al trattamento dei dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del 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 del 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 del GDPR**, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le **informazioni indicate dall'art. 14 del GDPR**, 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 "DPIA") ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

a) attribuire specifici compiti ed istruzioni, connesse al trattamento dei dati personali, a **soggetti "designati" che rivestono un elevato grado di responsabilità** all'interno dell'organizzazione aziendale, ossia a **tutti i Direttori/Dirigenti aziendali, Direttori di Dipartimento, Direttori di Presidio, Direttori di Distretto e Responsabili delle Strutture Complesse, Semplici e Semplici Dipartimentali**, 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) individuare le modalità più opportune per **autorizzare al trattamento dei dati personali le persone** che operano sotto la propria autorità diretta;
c) nominare il **Responsabile della protezione dei dati**;
d) nominare quale **Responsabile del trattamento** (ex art. 28 del GDPR) i soggetti esterni pubblici o privati affidatari di attività e servizi per conto dell'ASL di Foggia, relativamente alle banche dati gestite da soggetti esterni 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;

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ASL di Foggia 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 GDPR**. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di protezione dei dati personali, 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. Gli eventuali accordi di contitolarità saranno immediatamente notificati a tutti i Delegati al trattamento dei dati personali dell'ASL di Foggia.

8. **L'ASL di Foggia 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 del trattamento.

Art. 3 – Finalità del trattamento

I trattamenti sono compiuti dall'ASL di Foggia per le seguenti finalità:

a) tutela della salute, ossia **attività di diagnosi, assistenza e terapia sanitaria o sociale**;
b) attività **amministrativo, gestionali e contabili**, correlate alle prestazioni sanitarie erogate anche tramite Convenzioni con altre Strutture sanitarie autorizzate;
c) attività **socio-assistenziali** in favore di minori o soggetti non autosufficienti o incapaci;
d) attività di **programmazione, gestione, controllo e valutazione dell'assistenza sanitaria**;
e) attività legate alla **fornitura di beni o servizi all'utente** per la salvaguardia della salute (es. fornitura di ausili e protesi);
f) **adempimenti medico-legali**;

g) ai fini di implementazione dei **sistemi di sorveglianza e dei registri di patologia**;
h) **attività di ricerca medica, biomedica ed epidemiologica**;
i) ai fini dell'**attività didattica e formazione in campo universitario e professionale,** previa anonimizzazione dei dati;
j) **gestione, pianificazione e controlli dei rapporti tra l'ASL di Foggia e gli Enti accreditati o convenzionati con il SSN**;
k) per la gestione di **eventuali richieste risarcitorie**.

Ulteriori trattamenti, 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 **previo specifico consenso** dell'interessato, tra cui ad esempio:

l) Dossier Sanitario Elettronico e Fascicolo Sanitario Elettronico;
m) Refertazione on-line;
n) App mediche;
o) Medicina *c.d.* predittiva.

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'ASL di Foggia ritiene opportuno, alla luce della sua complessità organizzativa e della numerosità dei soggetti coinvolti nel trattamento dei dati, attribuire la delega di funzione a tutti i **Direttori/Dirigenti aziendali, Direttori di Dipartimento, Direttori di Presidio, Direttori di Distretto e Responsabili delle Strutture Complesse, Semplici e Semplici Dipartimentali**, per i trattamenti di rispettiva competenza, i quali potranno fornire idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

3. Ciascun **Delegato al trattamento dei dati**, **è nominato dal Direttore Generale quale responsabile dell'osservanza delle misure di sicurezza** fisiche, logiche ed organizzative previste dal Regolamento UE 2016/679 ed ai sensi dell'art. 2-quaterdecies del D.lg. 196/03, così come modificato dal D.lgs 101/18, con riferimento a tutte le

banche dati (in formato cartaceo ed elettronico) esistenti nell'articolazione organizzativa di rispettiva competenza. Con riferimento alle misure tecnologiche e di sicurezza informatica, adeguate al rischio insito nel trattamento dei dati, ai sensi dell'art. 32 del GDPR, ciascun "**Delegato al trattamento dei dati" è opportunamente supportato ed informato dalla S.S. Sistemi Informativi aziendali** che avrà predisposto tali misure direttamente o tramite società designate in qualità di Responsabili del trattamento. In allegato il modello di nomina del delegato interno al trattamento dei dati (ALL_1_Nomina-Delegato_Interno);

4. **L'autorizzazione generale al trattamento dei dati per tutto il personale aziendale è definita con la preposizione delle persone fisiche alle unità di trattamento per le quali è individuato l'ambito di trattamento consentito** e gli stessi sono raggruppati nelle seguenti principali classi omogenee:

   - dirigenti medici e veterinari;
   - dirigenti sanitari;
   - dirigenti appartenenti al ruolo amministrativo, tecnico e professionale;
   - personale infermieristico ed ostetrico;
   - personale tecnico/sanitario;
   - personale del ruolo professionale, tecnico ed amministrativo;
   - altri operatori del ruolo tecnico;
   - tirocinanti, frequentatori, stagisti, volontari;

Per la loro assegnazione sono individuate le seguenti principali Unità di trattamento:

- Presidio Ospedaliero
- Distretto Socio-Sanitario
- Dipartimento di Prevenzione, Dipartimento di Salute Mentale, Dipartimento Dipendenze Patologiche, Dipartimento di Medicina Fisica e Riabilitazione, Dipartimento di Emergenza-Urgenza
- Aree Aziendali
- Responsabili del trattamento (Terzi).

La matrice di designazione dei soggetti autorizzati per classi omogenee è riportata in allegato (All_5_Matrice-Preposizione-Autorizzati).

5. Ciascun "Delegato al trattamento dei dati" è tenuto altresì a nominare puntualmente i **soggetti autorizzati al trattamento dei dati, nella Struttura di propria competenza, impartendo istruzioni dettagliate e definendo gli ambiti di operatività consentiti** (accesso a banche dati, gestionali, cartelle cliniche elettroniche etc.) mediante

designazione individuale o collettiva come da fac-simile in allegato al presente Regolamento (allegati : All_3_Nomina_Collettiva-Autorizzati; All_4_Nomina_Individuale-Autorizzati).

6. Il "Delegato al trattamento dei dati" in conformità al GDPR provvede, per 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 della S.S. Sistemi informativi aziendali;
- alla rilevazione dei fabbisogni formativi 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, 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"), utilizzando il modello che si allega al presente atto per farne parte integrante e sostanziale (All_22_Modello Segnalazione Interna Data-Breach).
- richiedere agli uffici competenti la formalizzazione del contratto da cui scaturiscono gli obblighi ex art. 28 paragrafo 3 del Regolamento UE 2016/679 a carico dei Responsabili del trattamento, ossia dei soggetti pubblici o privati affidatari di attività e servizi per conto dell'ASL di Foggia, relativamente alle banche dati gestite da soggetti esterni 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";
- adottare, con riferimento ai rapporti in essere con i Responsabili del trattamento, ogni iniziativa utile ad acquisire notizie relative all'adeguamento della relativa struttura alle norme Regolamento UE 2016/679, ponendo a loro carico ogni ulteriore onere informativo e/o dichiarativo nei confronti dell'ASL di Foggia;

- individuare eventuali contitolari del trattamento, ai sensi dell'art. 26 del Regolamento UE 2016/679, qualora il trattamento sia effettuato in ottemperanza di norme regionali o nazionali richiedendo agli uffici competenti la predisposizione di atti giuridici necessari per individuare i distinti ruoli e responsabilità;
- vigilare sull'idoneità dell'informativa resa all'interessato rispetto al trattamento dei dati personali, adottando eventuali ulteriori misure necessarie per migliorare la comprensibilità della comunicazione;
- adottare misure organizzative ed operative adeguate per il soddisfacimento delle richieste di esercizio dei diritti riconosciuti all'interessato ed espressamente disciplinati agli artt. 12 e seguenti del Regolamento UE 2016/679.

7. **Il Titolare può avvalersi, per il trattamento di dati personali e particolari (ex sensibili), di soggetti esterni pubblici o privati che, in qualità di Responsabili del trattamento, ai sensi dell'art. 28 del GDPR, 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.

   Le Strutture aziendali preposte alla definizione delle procedure di gara (disciplinari/capitolati tecnici), convenzioni e comodati d'uso di prodotti, dispositivi e servizi che comportano il trattamento di dati personali di cui è Titolare l'ASL di Foggia, utilizzano il modello in allegato (All_23_Mod_Attestazione_Compliance) per verificare *ab origine* le garanzie offerte dal Partecipante in materia di protezione dei dati personali.

8. **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, GDPR**; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea. Ai fini della predisposizione di ciascun contratto con le terze parti potrà essere richiesto il supporto del Responsabile per la protezione dei dati dell'ASL di Foggia. In allegato un fac-simile da personalizzare in base al tipo di contratto stipulato con i terzi (ALL_2_Contratto_Responsabile_Art28).

9. 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. I nominativi di tali incaricati (soggetti autorizzati) e i relativi ambiti di intervento sono portati a conoscenza, per competenza, dei Delegati al trattamento dei dati dell'ASL di Foggia. 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.

10. 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.

Art. 5 – Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati è designato dal Titolare o suoi delegati, 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 GDPR 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 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 "Delegati per la protezione dei dati";

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA- *data protection impact assessment*) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD 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 del GDPR, 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) provvedere alla tenuta del registro delle attività di trattamento;

2. Il Titolare ed il "Delegati per la protezione dei dati" assicurano che il Responsabile della protezione dei dati (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. 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 GDPR 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'ASL di Foggia, in qualità di Titolare del trattamento, individua i soggetti operanti sulla rete informatica aziendale, in qualità di Amministratori di Sistema, per ambito di operatività consentito. Il Direttore Generale provvede a designare, tramite atto formale, le persone autorizzate con ruolo di amministratore di sistema, capaci cioè di accedere alla rete

informatica aziendale, agli apparati di rete, ai computer e server con privilegi amministrativi, per fini di manutenzione ed assistenza.

Nel caso di presenza di soggetti terzi (consulenti e fornitori) autorizzati all'erogazione di servizi di assistenza sistemistica ed applicativa, di gestione della sicurezza informatica e monitoraggio della rete informatica, il Direttore Generale o suo delegato individua la persona giuridica in qualità di Responsabile del trattamento con funzioni di amministratore di sistema, ai sensi dell'art. 28 del GDPR, con la formalizzazione di un contratto tra le parti, al fine di specificare i compiti e responsabilità.

Art. 7 – Informativa e Consenso

INFORMATIVA

L'ASL di Foggia, in qualità di Titolare del trattamento, predispone le **informative** 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'art. 13 del GDPR, 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 secondo il Piano di conservazione dell'ASL di Foggia (*c.d. massimario di scarto*) 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.

L'informativa è fornita agli Utenti, mediante idonei strumenti, quali:

a) **moduli appositi (**informativa sintetica come da allegato All_8_Informativa-Sintetica-Assistiti) da consegnare **agli interessati**. Nel modulo sono riportate informazioni sintetiche, ivi compresi i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti. Tale informativa rinvia all'informativa estesa (dettagliata) consultabile sul sito web istituzionale;

b) **cartelli agevolmente visibili dal pubblico**, posti nei locali di accesso delle strutture dell'Azienda, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet dell'Azienda;

c) **avvertenza apposita** inserita nei contratti o nelle lettere di affidamento al servizio del personale dipendente, del personale medico convenzionato, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, degli specializzandi, tirocinanti, dei volontari, ecc. Per quanto riguarda i soggetti che hanno già instaurato rapporti con l'ASL di Foggia, l'informativa è fornita nei tempi e nei modi che saranno concordati con il Responsabile della protezione dei dati;

d) **avvertenza resa in sede di pubblicazione dei bandi**, con l'indicazione del responsabile del trattamento dei dati relativi alle procedure concorsuali, all'affidamento di lavori o gare di forniture di beni e di servizi.

Ai sensi dell'art. 79 del vigente Codice in materia di protezione dei dati personali, con riguardo alle prestazioni sanitarie e socio-sanitarie, le articolazioni aziendali annotano l'avvenuta informazione, ove possibile e tramite procedure informatizzate, con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

CONSENSO

Per le finalità di trattamento indicate nell'art. 3 ai p.ti ad a) a k), ai fini dell'esecuzione di compiti di interesse pubblico rilevante, connessi all'esercizio di pubblici poteri e sulla base di una norma di legge o di regolamento, il **consenso dell'interessato non è dovuto**.
Il trattamento dei dati personali, per le **finalità indicate nell'art. 3 ai p.ti ad l) a o)**, il **consenso dell'interessato è dovuto.**

Il consenso dell'interessato è dovuto anche per le eventuali comunicazioni a soggetti terzi del suo stato di salute e sulla sua presenza/dislocazione nei reparti durante il ricovero presso le strutture dell'ASL di Foggia. Il consenso acquisito dall'interessato, in regime di ricovero o per le finalità di cui all'art. 3 ai p.ti l) a o), con modalità manuale cartacea o informatica, potrà restare valido anche per tutti i successivi eventuali accessi dell'assistito presso le strutture sanitarie dell'ASL di Foggia, anche in tempi diversi, fino ad esplicita revoca del consenso medesimo da parte dell'interessato.

Ciascun Delegato al trattamento dei dati (tutti i Direttori/Dirigenti aziendali, Direttori di Dipartimento, Direttori di Presidio, Direttori di Distretto e Responsabili delle Strutture Complesse, Semplici e Semplici Dipartimentali) si impegna a fornire agli Assistiti le informazioni sul trattamento dei dati, ai sensi degli artt. 13-14 del Regolamento UE 2016/679, che si allegano al presente Regolamento, come di seguito meglio specificato :

- All_6-Informativa-Assistiti-Prestazioni: da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI. Tale informativa dovrà essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;

- All_8_Informativa-Sintetica-Assistiti: da inserire nelle cartelle cliniche e da consegnare all'assistito ad ogni sua esplicita richiesta.

- All_7_Informativa-Assistiti-Refertazione: da utilizzare nell'ambito del servizio specifico di refertazione on-line ove il consenso informato al trattamento dei dati dovrà essere acquisito obbligatoriamente attraverso procedure manuali o informatizzate.

- All_9_Informativa-Poster-Assistiti-Prestazioni: da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero/ambulatoriale/ALPI tramite affissione dei cartelli nelle sale d'attesa dei reparti e nei locali di affluenza del pubblico;

- All_10_Informativa-Assistiti-Amministrativo:

da utilizzare nell'ambito delle attività amministrative correlate alle prestazioni sanitarie (CUP, URP etc.). Tale informativa dovrà :

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere fornita all'assistito ad ogni sua esplicita richiesta.

- All_11_Informativa-Poster-Assistiti-Amministrativo: da utilizzare nell'ambito delle attività amministrative correlate alle prestazioni sanitarie (CUP, URP etc.) tramite affissione di cartelli nei locali di affluenza del pubblico;
- All_21_Consenso-Ricoveri: da utilizzare nell'ambito delle prestazioni sanitarie offerte in regime di ricovero, da far compilare e firmare all'Assistito o suo rappresentante legale e da custodire in cartella clinica.

- ALL_12_INFORMATIVA-DS-FSE

Tale informativa dovrà:

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere fornita all'Assistito ad ogni sua esplicita richiesta nell'ambito del trattamento dei dati con Dossier e/o Fascicolo Sanitario Elettronico.

- ALL_13_INFORMATIVA-DIPENDENTI

Tale informativa dovrà:

- essere consultabile dal sito internet istituzionale o intranet a tutto il personale aziendale;
- essere fornita al dipendente ad ogni sua esplicita richiesta nell'ambito del trattamento dei suoi dati per le finalità di gestione del rapporto di lavoro.

- ALL_14_INFORMATIVA-GARE-CONTRATTI-INCARICHI

Tale informativa dovrà :

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere fornita nell'ambito del trattamento dei dati di partecipanti a gare, contratti o affidamento di incarichi.

- ALL_15_INFORMATIVA-ASSISTITI-SERVIZI-ONLINE

Tale informativa dovrà:

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere accessibile con riferimento a tutti i servizi erogati on-line attraverso il sito internet istituzionale.

- ALL_16_INFORMATIVA-CONCORSI

Tale informativa dovrà:

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere fornita a tutti i partecipanti a bandi di concorso avviati dall'ASL di Foggia.

- ALL_17_INFORMATIVA-EVENTI-CONGRESSI

Tale informativa dovrà:

- essere consultabile dal sito internet istituzionale, in apposita sezione Privacy;
- essere fornita a tutti i partecipanti agli eventi organizzati dall'ASL di Foggia.

- ALL_18_MODELLO-RECLAMO-GARANTE

Tale modulo dovrà essere:

- pubblicato sul sito internet istituzionale per garantire l'esercizio del diritto di reclamo all'Autorità Garante da parte dell'interessato;
- inviato su richiesta esplicita dell'interessato.

- ALL_20_Modulo_ESERCIZIO_DIRITTI

Tale modulo dovrà essere:

- pubblicato sul sito internet istituzionale per garantire l'esercizio di tutti i diritti dell'interessato di cui agli artt. 15-22 del Regolamento UE 2016/679;
- inviato su richiesta esplicita dell'interessato.

Ciascun Delegato al trattamento dei dati dovrà predisporre e rendere le informative Privacy nel caso di trattamenti specifici di dati personali, utilizzando il modello fac-simile in allegato per le personalizzazioni del caso (allegato: ALL_19_INFORMATIVE-CUSTOM).
La modulistica inerente la protezione dei dati personali dovrà essere sempre consultabile e facilmente accessibile tramite il sito internet aziendale, nell'apposita sezione Privacy.

Art. 8 – I diritti degli interessati

L'ASL di Foggia garantisce l'esercizio dei diritti degli interessati individuando nei **Delegati al trattamento dei dati**, designati con atto individuale dal Direttore Generale (tutti i Direttori/Responsabili di Struttura semplice, complessa e dipartimentale), i **Referenti per il riscontro all'interessato**, nei termini previsti dalla norma.
Gli interessati possono contattare, ove necessario, il Responsabile della protezione dei dati dell'ASL di Foggia per l'esercizio dei loro diritti. L'interessato ha il diritto di ottenere dall' ASL di Foggia 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 dell'ASL di Foggia 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'ASL di Foggia 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' ASL di Foggia, 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' ASL di Foggia.

Art. 10 – Liceità del trattamento

I dati personali possono essere trattati soltanto:

- da parte del Titolare, dei Contitolari, dei Delegati per la protezione 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 ambito genetico e della medicina predittiva, in caso di utilizzo di dossier o fascicolo sanitario elettronico*), è compito dell' ASL di Foggia 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, ove richiesto, al fine anche di consentire un agevole esercizio dei diritti degli interessati.

Art. 11 – Sicurezza del trattamento

1. L' ASL di Foggia e **ciascun "Delegato al trattamento dei dati" mettono in atto misure tecniche ed organizzative adeguate, con il supporto e sotto la responsabilità della S.S. Sistemi informativi Aziendali e dell'Area Gestione Tecnica nell'ambito delle rispettive competenze**, 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 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. L' ASL di Foggia e ciascun "Delegato al trattamento dei dati" in conformità al GDPR 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'ASL di Foggia.

6. I nominativi ed i dati di contatto del Titolare, dei "Delegato al trattamento dei dati", dei Responsabili del trattamento ex art. 28 del GDPR, dei conTitolari e del Responsabile della protezione dati, sono pubblicati sul sito istituzionale dell'ASL di Foggia, nell'apposita sezione Privacy.

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'ASL di Foggia, predispone il Registro delle attività di trattamento, con piattaforma informatica collaborativa, 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.

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 sulla protezione dei dati

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 sulla protezione dei dati 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 dall'Autorità Garante per la protezione dei dati, ai sensi dell'art. 35, pp. 4-6 del 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 del 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 del 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 dell'ASL di Foggia, soggetti con patologie psichiatriche, 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 all'organizzazione.

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

   Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile dei Sistemi Informativi Aziendali fornisce supporto al Titolare per lo svolgimento della DPIA, ove necessario.

5. Il RPD 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 S.S. Sistemi informativi aziendali può 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 del 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 dell'Autorità Garante prima del mese di 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.

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 dell'Autorità Garante;

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 l'Autorità Garante prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta l'Autorità Garante 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. 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 da tutto il personale dell'ASL di Foggia.

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità 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", in conformità al GDPR, 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, all'indirizzo email databreach.pa@pec.gpdp.it**.**

2. 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.

3. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorità 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.

4. 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.
5. 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.

6. 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 l'Autorità Garante e l'interessato, se del caso.
7. 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 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 all'Autorità Garante che il *data-breach* non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

8. Ogni Delegato al trattamento dei dati, ciascuno per il proprio ambito di competenza, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 12 ore, la violazione dei dati rilevata ai soggetti di seguito elencati:

- **Direttore Generale**
- **Responsabile della protezione dei dati**
- **Responsabile dei Sistemi informativi aziendali**

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 (ALL_22_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**
- **Direttore Amministrativo**
- **Responsabile della protezione dei dati**
- **Responsabile Sistemi informativi aziendali**
- **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.

9. 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.

10. 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 20.000.000 di euro.

Art. 15 – Rinvio

Per quanto non espressamente previsto nel presente Regolamento si fà rinvio al Regolamento UE 679/2016 e al D.lgs. n. 196/03, così come modificato dal D.lgs 101/18.

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

Allegati disponibili su intranet aziendale:

- All_1_Nomina-Delegato_Interno
- All_2_Contratto_Responsabile_Art28
- All_3_Nomina_Collettiva-Autorizzati
- All_4_Nomina_Individuale-Autorizzati
- All_5_Matrice-Preposizione-Autorizzati
- All_6-Informativa-Assistiti-Prestazioni
- All_7_Informativa-Assistiti-Refertazione
- All_8_Informativa-Sintetica-Assistiti
- All_9_Informativa-Poster-Assistiti-Prestazioni
- All_10_Informativa-Assistiti-Amministrativo
- All_11_Informativa-Poster-Assistiti-Amministrativo
- All_12_Informativa-Ds-Fse
- All_13_Informativa-Dipendenti
- All_14_Informativa-Gare-Contratti-Incarichi
- All_15_Informativa-Assistiti-Servizi-Online
- All_16_Informativa-Concorsi
- All_17_Informativa-Eventi-Congressi

- All_18_Modello-Reclamo-Garante
- All_19_Informative-Custom
- All_20_Modulo_Esercizio_Diritti
- All_21_Consenso-Ricoveri
- All_22_Modello segnalazione interna data-breach
- All_23_Mod_Attestazione_Compliance