SISTEMA DI GESTIONE DEI TRATTAMENTI
ai sensi del Regolamento (UE) 2016/679

MANUALE

Identificativo documento	Sistema di Gestione dei Trattamenti
Versione	00
Data Approvazione	
Redatto da	CO.DE S.r.l.
Verificato	
Approvato	

REVISIONI

Versione	Data	Contenuto
00		Prima emissione

SISTEMA DI GESTIONE DEI TRATTAMENTI AI SENSI DEL REGOLAMENTO UE 2016/679

MANUALE

INDICE

1. IL REGOLAMENTO (UE) 2016/679 e il D.LGS. 101/2018..... 3
1.1. Il regime di applicabilità del Regolamento UE 2016/679 3
1.2. I principi del Regolamento (UE) 2016/679 4
1.3. Gli adempimenti a carico degli Ordini Professionali 14

2. I SOGGETTI DEL TRATTAMENTO..... 15
2.1. Titolare del trattamento 16
2.2. Contitolare del trattamento 18
2.3. Responsabile del trattamento dei dati 18
2.4. Destinatario 19
2.5. Designati o autorizzati al trattamento dei dati personali 19
2.6. Interessati 19
2.7. Responsabile della Protezione dei Dati 20
2.8. Rappresentante nell'Unione dei Titolari o dei Responsabili del trattamento 20
2.9. Autorità di controllo 20
2.10. Comitato Europeo per la protezione dei dati 20

3. NATURA ED ORGANIZZAZIONE DELL'ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI FOGGIA 21
3.1. La natura dell'Ordine delle Professioni Infermieristiche di Foggia e le sue funzioni 21
3.2. Struttura organizzativa 22

4. LA FIGURA DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI..... 23
4.1. Designazione del DPO 23
4.2. Requisiti 25
4.3. Nomina, durata e revoca 25
4.4. Compiti del DPO 26
4.5. Poteri 27
4.6. Funzionamento del DPO 27
4.7. Flussi informativi verso il Titolare e il Responsabile del Trattamento 27
4.8. Flussi informativi verso il DPO 28

5. ADOZIONE DEL SISTEMA DI GESTIONE DEI TRATTAMENTI DA PARTE DELL'ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI FOGGIA 29
5.1. Obiettivi perseguiti con l'adozione del Sistema 29
5.2. La metodologia seguita nella costruzione del Sistema 29

5.3. Funzione del Sistema 30
5.4. Struttura del Sistema di gestione 30

6. FORMAZIONE ED INFORMAZIONE 32

6.1. Formazione del dipendente di OPI Foggia 32
6.2. Contenuti della formazione ed informazione 33

7. ANALISI DEI RISCHI 33

7.1. Premessa 33
7.2. Attività di analisi dei rischi 34
7.3. *FMEA - Failure Mode and Effect Analysis* 35

1. IL REGOLAMENTO (UE) 2016/679 e il D.LGS. 101/2018

1.1. Il regime di applicabilità del Regolamento UE 2016/679

Il Regolamento (UE) 2016/679 - del Parlamento Europeo e del Consiglio - per la Protezione dei Dati o *GDPR* (acronimo di: *General Data Protection Regulation*) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è stato emanato il 27 aprile 2016 e pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 4 maggio 2016.

Successivamente, con il D.Lgs. 10 agosto 2018 n.101 (vigente a far data dal 19.09.2018), in attuazione della legge delega 25 ottobre 2017 n.163, sono state emanate disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.

Il nuovo regolamento –in vigore a partire dal 25 maggio 2018– si articola in 11 capi per un totale di 99 articoli.

La parte dispositiva è preceduta da ben 173 "*considerando*" i quali chiariscono il contesto e le ragioni della nuova normativa.

Particolarmente interessante è il *considerando* 9, nel quale il legislatore comunitario riconosce espressamente che la Direttiva 95/46/CE «*non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione (...) che (...) le operazioni online comportino rischi per la protezione delle persone fisiche*».

Le divergenze nell'attuazione e nell'applicazione della Direttiva 95/46/CE all'interno degli ordinamenti giuridici dei singoli Stati membri hanno così dato luogo alla «*compresenza di diversi livelli di protezione (...) dei dati personali*» e ciò, secondo il legislatore comunitario, può ostacolare la libera circolazione di tali dati all'interno dell'Unione e «*costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione*».

Non è però soltanto a questi inconvenienti che si è inteso ovviare con l'emanazione del nuovo regolamento.

Infatti, l'esigenza di una riforma della materia è sorta anche e soprattutto dalla continua evoluzione degli stessi concetti di *privacy* e di *data protection*, dovuta principalmente all'incessante progresso dei servizi *on line*.

La precedente Direttiva 95/46/CE era stata adottata nel 1995 con due principali obbiettivi:

1) salvaguardare il diritto fondamentale dei soggetti alla protezione dei dati;
2) garantire la libera circolazione dei dati personali fra gli Stati membri.

Negli anni immediatamente successivi, l'entità fenomenica della condivisione e della raccolta di dati è aumentata in modo vertiginoso soprattutto a seguito dello sviluppo delle nuove tecnologie.

Tutto ciò ha finito col mettere inesorabilmente in luce l'inidoneità del quadro normativo offerto dalla direttiva del 1995, pur rimanendone validi gli obiettivi e i principi di fondo.

È divenuto necessario, quindi, instaurare un quadro giuridico più solido e coerente, adeguato allo sviluppo dell'economia digitale nel mercato interno.

1.2. I principi del Regolamento (UE) 2016/679

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali, consacrando il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla autodeterminazione informativa.

Si passa in tal modo da un diritto alla protezione dei dati personali di tipo *nazionale e individuale* ad un diritto di tipo *europeo e sociale*.

In generale, il Regolamento:

a) muta l'approccio regolatorio da "*formale e re-attivo*" in "*sostanziale e pro-attivo*": il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali di un ente o di un'azienda;
b) consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni: riaffermazione di molti principi già disciplinati in ambito europeo (ad esempio diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione), rafforzamento di altri (disciplina del consenso del quale introduce un vera e propria definizione dell'istituto del "*consenso esplicito*" e della "*trasparenza*" rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa), introduzione di nuovi (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
c) accresce le responsabilità del titolare e del responsabile mediante il principio di *accountability* con l'obiettivo di ridurre i rischi di operazioni non conformi o non consentite;
d) centralizza la *governance* e il controllo sul rispetto e la conformità dei trattamenti alla normativa, ampliando il sistema vigilanza e rafforzando quello sanzionatorio.

Nella PA, l'atteggiamento rispetto al trattamento dei dati e delle banche dati è molto cambiato negli ultimi 20 anni, da mero adempimento si è passati ad una dimensione molto più proattiva, perché i dati e talora anche i dati personali escono sempre di più dagli uffici attraverso processi legislativi che tengono conto del loro valore economico.
La PA, che fino a qualche tempo fa, gestiva passivamente i dati, oggi vuole -e deve- renderli sempre più disponibili e trasparenti.
Le stesse considerazioni valgono anche per gli Ordini Professionali poichè sottoposti ai medesimi obblighi di trasparenza previsti per le pubbliche amministrazioni in quanto compatibili (art. 2- bis, co.2, lett. a) del D.lgs. 33/2013).
Ciò determina spesso inevitabili conflitti fra *privacy* e trasparenza amministrativa specialmente alla luce delle disposizioni di cui al d.lgs. n. 33/2013 che nel disciplinare il riutilizzo dei dati pubblicati regola necessariamente i rapporti con la normativa in materia di protezione dei

dati personali chiarendo che gli obblighi di pubblicazione dei dati personali diversi dai dati particolari, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca *web* ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.
La norma ancora prevede che nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, particolari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.
Con l'adozione di apposite Linee guida (provvedimento del 15 maggio 2014), il Garante è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul *web* di atti e documenti.
Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti *web* istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.
Dopo aver verificato la sussistenza dell'obbligo di pubblicazione dell'atto o del documento nel proprio sito *web* istituzionale, il soggetto pubblico deve limitarsi a includere negli atti da pubblicare solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto. Se si tratta di dati particolari (ossia idonei a rivelare ad esempio l'origine razziale ed etnica, le convinzioni religiose, le opinioni politiche, l'adesione a partiti o sindacati, lo stato di salute e la vita sessuale) o relativi a procedimenti giudiziari, i dati possono essere trattati solo se indispensabili, ossia se la finalità di trasparenza non può essere conseguita con dati anonimi o dati personali di natura diversa.
Per la trasparenza c'è bisogno di un approccio qualitativo e non meramente quantitativo: meno dati ma più qualificati.
In un ambito pubblicistico, il concetto di trasparenza è sicuramente collegato a quello di *accountability*, uno dei principi fondamentali del GDPR.
L'*accountability*, difatti, si compone di almeno tre elementi:

1. La "*trasparenza*" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.
2. La "*responsività*" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli *stakeholder*.
3. La "*compliance*" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori della PA.

1.2.1. Ambito di territorialità

Il Regolamento (cfr. considerando da 14 a 27 e art. 3) supera il criterio dello stabilimento e si applica al trattamento dei dati personali da parte di titolari anche non stabiliti nel territorio dell'Unione purché il trattamento riguardi l'offerta di beni, servizi o il monitoraggio del comportamento del soggetto interessato aventi luogo nell'Unione.

Si rileva, inoltre, che le disposizioni del regolamento trovano applicazione a qualsiasi forma di trattamento automatizzato di dati personali, nonché al trattamento non automatizzato di dati personali contenuti in un archivio (cfr. art. 2).

1.2.2. Responsabilità dei titolari e dei responsabili del trattamento

Il Regolamento ha accentuato il profilo di responsabilità dei Titolari (cfr. art. 24 e 25) e del Responsabile del Trattamento (cfr. art. 28), prevedendo la predisposizione di misure tecnico/organizzative adeguate onde garantire la conformità del trattamento dei dati alla normativa vigente.

A tali figure si affianca quella del Responsabile della Protezione dei dati personali (c.d. "*data protection officer*" o DPO).

Rientrano tra le responsabilità del Titolare e dei Responsabili del trattamento quelle attinenti:

- l'attuazione dei principi di *privacy by design e by default*;
- la *valutazione d'impatto* (*DPIA*);

- la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi;
- la tenuta dei rispettivi registri delle attività di trattamento;
- la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato.

1.2.3. Rafforzamento delle tutele riservate all'interessato

Aspetto rilevante concerne la previsione di misure di sicurezza e delle misure di tutela e garanzia dell'interessato nel trattamento dei suoi dati mediante:

a. <u>Principio della *Privacy by design*</u>

Implica che la protezione dei dati sia integrata nell'intero ciclo di vita di una data tecnologia o servizio o processo, sin dalla relativa progettazione. In altre parole, qualsiasi progetto deve essere realizzato avendo presente, sin dal principio – *by design*, appunto – la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto (informatiche e non).

Le misure strumentali a tale scopo sono:

- la migliore applicazione del principio di minimizzazione dei dati personali oggetto del trattamento con riferimento alla quantità dei dati, ai tempi di conservazione, ai livelli di accessibilità e alle prefissate finalità;
- la pseudonimizzazione ovvero l'oscuramento (reversibile) dei dati identificativi del soggetto interessato.

b. <u>Principio della *Privacy by default*</u>

Il principio della *privacy by default* implica che i dati vengano raccolti nella minore misura possibile e che le finalità del trattamento siano quanto più possibile limitate.

In tal modo, il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate onde garantire che siano trattati, per impostazione predefinita (di *default*), solo i dati personali necessari

per ogni specifica finalità del trattamento (che non risultino pertanto eccedenti rispetto al ruolo del soggetto che li tratta).

c. <u>Valutazione di impatto (*DPIA*)</u>

La valutazione d'impatto è finalizzata a stimare la gravità del rischio, ed è richiesta per trattamenti su larga scala che incidono su un vasto numero di interessati, con un elevato rischio connesso all'introduzione di nuove o particolari tecnologie, all'implementazione di trattamenti di profilazione o di sorveglianza o all'utilizzo di particolari dati (biometrici o giudiziari).

La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità;
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le previste misure organizzative e tecniche (comprese quelle di sicurezza) e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

d. <u>Sicurezza e valutazione dei rischi</u>

Il Regolamento UE prevede l'adozione di misure di sicurezza idonee in relazione alla valutazione dei rischi.

Titolare e Responsabile del Trattamento sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono:

- la pseudonimizzazione dei dati;
- la cifratura dei dati;
- misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
- la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Tali misure vanno modellate in base al contesto e alla finalità di trattamento.

e. Notifica nell'ipotesi di violazione dei dati personali

Il Regolamento UE equipara la violazione dei dati personali affiancando alla tradizionale componente dolosa quella accidentale prevedendo analoghe implicazioni.

La violazione del dato personale viene definita ai sensi dell'articolo 4, paragrafo 1, n. 12 come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Il Titolare deve comunicare all'Autorità di Controllo l'avvenuta violazione dei dati personali trattati entro e non oltre 72 ore dall'acquisizione della conoscenza dell'accadimento descrivendone:

- la natura della violazione, le categorie e il numero approssimativo degli interessati e delle registrazioni dei dati personali;
- i dati di contatto del responsabile della protezione dei dati;
- le probabili conseguenze della violazione;
- le misure adottate o che si intendono adottare per rimediare la violazione o attenuarne gli effetti negativi.

Oltre alla comunicazione all'Autorità di Controllo, la violazione deve essere comunicata anche all'interessato se la violazione è suscettibile di elevati rischi per i diritti e le libertà dell'interessato (art. 34 del GDPR).

f. Introduzione dei registri delle attività di trattamento

Il Titolare e il Responsabile del trattamento devono tenere i rispettivi registri delle attività di trattamento.

Il registro del Titolare deve contenere:

- riferimenti di contatto del Titolare/i, del rappresentante del Titolare del trattamento nell'Unione Europea (in caso di non stabilimento nell'Unione) e del Responsabile della protezione dei dati;
- le finalità;

- descrizione degli interessati e dei destinatari;
- la categoria dei dati personali trattati;
- la presenza di trasferimenti di dati verso un Paese Terzo, un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie;
- la tempistica della cancellazione dei dati;
- la descrizione delle misure di sicurezza e organizzative adottate.

Il registro del Responsabile deve contenere:

- la tempistica della cancellazione dei dati;
- la descrizione delle misure di sicurezza e organizzative adottate;
- i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto del Titolare.

g. <u>Smaltimento di dispositivi e supporti contenenti dati personali</u>

Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono.

1.2.4. Consenso

Il consenso in generale deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto.

Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente. Non è richiesta necessariamente la forma scritta anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito.

Si precisa che, nel caso il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto.

Per il trattamento di categorie particolari di dati è necessario il consenso [cfr. art. 9 par. 2 lett. a)] a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso [cfr. art. 9 par. 2 lett. c, f, g, i, j].

1.2.5. Informativa

Il titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (cfr. art. 13 par. 4) o in altri casi particolari descritti dal Regolamento (art. 14 paragrafo 5).

Contenuto dell'informativa

L'informativa dovrà indicare:

- l'identità e i dati di contatto del Titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal titolare del trattamento o da terzi [qualora trovi applicazione l'art. 6 par. 1, lettera f)];
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventualità che il Titolare del trattamento trasferisca i dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati personali oppure, ove non sia possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato;

- la necessità di comunicare i dati personali e la fonte del relativo obbligo.

Caratteristiche dell'informativa

Il Regolamento UE specifica in dettaglio le caratteristiche espositive dell'informativa, precisando che deve essere:

- concisa;
- trasparente;
- intelligibile per l'interessato;
- facilmente accessibile;
- veicolata da un linguaggio chiaro e semplice.

1.2.6. I diritti dell'interessato

Diritti "tradizionali"

I diritti azionabili dall'interessato - già disciplinati dalla previgente normativa europea e nazionale - hanno ad oggetto:

- il diritto di accesso;
- la rettifica;
- la cancellazione;
- l'opposizione al trattamento.

Il Regolamento (EU) prevede altresì:

- diritto di limitazione;
- diritto di opposizione alla profilazione;
- diritto alla cancellazione/all'oblio;
- diritto alla portabilità.

1.3. Gli adempimenti a carico degli Ordini Professionali

Il GDPR non prevede una specifica disciplina per il trattamento dei dati personali effettuato dai soggetti pubblici e quindi dagli Ordini Professionali.

In realtà, non contiene una formale bipartizione tra titolari pubblici e privati e non contiene nemmeno norme specifiche dedicate al settore privato e pubblico ma si occupa in generale delle condizioni di liceità del trattamento (cfr. **art. 6 e art. 9, comma 2**, in relazione ai dati particolari), anche se poi alcune di esse riguardano esclusivamente lo svolgimento di attività pubbliche.

Il Regolamento, quindi, non si sofferma sulla natura pubblica o privata del titolare del trattamento, ma sulla tipologia di trattamento, che scaturisce dall'attività svolta dal titolare.

Non contiene neppure la suddivisione tra condizioni di liceità applicabili a soggetti privati e condizioni valide per i soggetti pubblici, come accadeva con il Capo II del Codice Privacy, dove, ad eccezione del settore sanitario, si menzionava l'istituto del consenso quale elemento distintivo tra titolari privati e titolari pubblici.

In effetti, tra gli stessi presupposti di liceità del trattamento dei dati personali il GDPR all'**art. 6, lett. e)** fa riferimento alla necessarietà del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, caso tipico, naturalmente dell'ente pubblico.

Si pensi, poi, all'**art. 9 del GDPR** che tra le eccezioni al divieto generale di trattare dati personali particolari fa rientrare:

- il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e

prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

- il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, o comunque necessario per motivi di interesse pubblico nel settore della sanità pubblica;
- il trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

L'**art. 10 del GDPR**, poi, con riferimento al **trattamento dei dati giudiziari** chiarisce che lo stesso deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Anche un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Altra norma di sicuro interesse per l'indubbia rilevanza in materia pubblicistica è rappresentata dall'**art. 23 del GDPR** che chiarisce come il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento possa limitare, mediante specifiche misure legislative, la portata di alcuni fondamentali obblighi e diritti degli interessati qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare tra gli altri anche finalità di pubblico interesse.

2. I SOGGETTI DEL TRATTAMENTO

Il Regolamento individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali i dati sono raccolti. In particolare:
   - il **Titolare**;
   - il **Contitolare**;

- il **Responsabile del trattamento**;
- il **Destinatario**;
- il **soggetto autorizzato o designato**;
- l'**interessato**;

2) delle caratteristiche del trattamento, delle tipologie e quantità di dati trattati. In particolare:
   - il **Responsabile della Protezione dei Dati** (***RPD*** **o** ***DPO***);

3) dell'ambito territoriale. In particolare:
   - il **Rappresentante nell'Unione dei Titolari o dei Responsabili del trattamento**;
   - l'**Autorità di Controllo;**
   - il **Comitato Europeo per la Protezione dei Dati.**

Nell'ambito aziendale la distribuzione dei ruoli e delle responsabilità costituisce una misura di sicurezza essenziale per l'applicazione delle disposizioni del Regolamento.

2.1. Titolare del trattamento

Il Titolare è definito all'art. 4 n.7 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

Pertanto, il Titolare non viene designato o nominato ma assume tale veste nel momento in cui raccoglie i dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

- determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue l'Ordine Professionale degli Infermieri, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali (art. 4);
- mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. *accountability*) (art. 24);
- garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
- individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
- agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
- designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
- istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
- effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
- comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
- ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
- rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
- rispondere delle violazioni amministrative ai sensi del GDPR (art. 83).

Nel nostro caso, il Titolare del Trattamento, è l'ordine delle Professioni Infermieristiche di Foggia.

2.2. Contitolare del trattamento

Il contitolare ai sensi dell'art. 26 è la persona fisica o giuridica che determina, congiuntamente ad un altro o più titolari del trattamento, le finalità e i mezzi del trattamento stesso.

2.3. Responsabile del trattamento dei dati

Il Responsabile del Trattamento trova definizione nell'art. 4 come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Le relative funzioni sono indicate nell'art. 28.

Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative di cui all'art. 5 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. E' consentita la nomina di sub-responsabili del trattamento (gli incaricati del trattamento nel Codice Privacy) 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'inadempimento, 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 sul suo operato.

2.4. Destinatario

L'art. 4 definisce destinatario "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi*".

Quindi, debbono essere considerati destinatari tutti i soggetti che ricevono dati personali da un titolare, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare, sia che li ricevono per conseguire proprie finalità.

Qualora il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie offerte da questi per la protezione dei dati siano adeguate.

2.5. Designati o autorizzati al trattamento dei dati personali

L'art. 29 "*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*" prevede che "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*"

Tale previsione si concretizza con l'individuazione dei soggetti autorizzati al trattamento dei dati.

È necessario, pertanto, che il Titolare, organizzi al proprio interno una distribuzione delle responsabilità rispetto al trattamento dati, delegando ed istruendo tutti coloro che dirigono strutture interne.

2.6. Interessati

L'interessato (*data subject*) è la persona fisica alla quale si riferiscono i dati trattati.

In altre parole, è il soggetto "proprietario" dei dati personali trattati, in relazione ai quali può esercitare importanti diritti disciplinati dal Regolamento.

2.7. Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati (*Data Protection Officer* siglabile in *D.P.O.*) è la persona giuridica, la persona fisica, l'autorità pubblica o altro organismo pubblico, eccettuate le Autorità Giurisdizionali nell'esercizio delle loro funzioni giurisdizionali, che monitora gli adempimenti sottesi all'applicazione del Regolamento per conto del Titolare o Responsabile del trattamento.

2.8. Rappresentante nell'Unione dei Titolari o dei Responsabili del trattamento

Il Rappresentante nell'unione dei Titolari o dei Responsabili di trattamento è definito dall'art. 4 "*La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento*".

2.9. Autorità di controllo

Trattasi dell'Autorità Pubblica indipendente istituita da uno stato membro ai sensi dell'art. 51.

2.10. Comitato Europeo per la protezione dei dati

Trattasi della persona giuridica col compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione (cfr. art. 68).

3. NATURA ED ORGANIZZAZIONE DELL'ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI FOGGIA

3.1. La natura dell'Ordine delle Professioni Infermieristiche di Foggia e le sue funzioni

L'Ordine delle Professioni Infermieristiche di Foggia -OPI- è un ente pubblico non economico, dotato di autonomia patrimoniale, finanziaria regolamentare e disciplinare, posto sotto la vigilanza del Ministero della Salute e coordinato nell'attività istituzionali dalla Federazione Nazionale Ordini delle Professioni Infermieristiche.

La sua *mission* è la tutela della professione infermieristica, del cittadino e della salute pubblica e la rappresentanza professionale degli iscritti ai propri Albi. Le funzioni di tutela e rappresentanza vengono sviluppate nell'interesse dei cittadini fruitori dell'assistenza infermieristica e dei professionisti infermieri la cui competenza e correttezza comportamentale è certificata dall'iscrizione al proprio Albo professionale a cui i professionisti infermieri hanno l'obbligo di essere iscritti per esercitare la propria attività di professionista, tutto ciò secondo le normative vigenti.

L'OPI di Foggia si occupa:

- Della gestione delle iscrizioni/cancellazioni dei professionisti all'albo;
- Dell'aggiornamento annuale dell'albo;

- Della gestione degli esposti pervenuti e della conseguente irrogazione di sanzioni disciplinari commisurate alla gravità della violazione commessa;
- Dell'organizzazione di corsi di formazione professionale rivolti ai propri iscritti e dell'assegnazione di crediti formativi.

I trattamenti sono compiuti dall'OPI:

1. per l'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
   - L'aggiornamento dell'Albo degli Infermieri;
   - Il conseguimento dei fini istituzionali dell'Ordine;
   - L'esercizio del potere disciplinare;
   - L'erogazione di servizi ai quali l'Ordine è tenuto;
   - Gli adempimenti di legge;
   - La gestione amministrativa del rapporto di iscrizione all'Ordine;
   - La formazione obbligatoria.
2. Per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

3.2. Struttura organizzativa

L'OPI Foggia con sede in Viale Giotto n.200, Foggia, ha come organizzazione interna:

- Un **Consiglio Direttivo**, che rappresenta l'organo di governo, composto da un Presidente, un Vicepresidente, un tesoriere, un Segretario ed 11 Consiglieri;

- Un **collegio di revisori dei conti**, costituito da tre membri effettivi ed un supplente.

Ciò posto, il Sistema *Privacy* di OPI Foggia è caratterizzato dalle seguenti figure:

a) Titolare dei trattamenti;
b) Responsabili dei trattamenti;
c) Soggetti interessati.

Il sistema di *governance privacy* dell'Ordine delle Professioni Infermieristiche di Foggia è illustrato nell'organigramma allegato al presente documento (**ALL. n.1**), nel quale sono rappresentate le diverse funzioni responsabili che caratterizzano la struttura operativa.

*** * ***

4. LA FIGURA DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

4.1. Designazione del DPO

L'art. 37, paragrafo 1, lett. a) - c) del GDPR, ha previsto l'obbligatoria istituzione di tale figura nelle ipotesi in cui:

a) il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali che espletino funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Pur non essendo prevista dal GDPR una definizione *ad hoc* di "autorità pubblica" o di "organismo pubblico", si legge nelle *FAQ* sul Responsabile della Protezione dei Dati in ambito pubblico pubblicate sul sito del Garante Privacy che "*devono ritenersi tenuti alla designazione di un RPD i soggetti che ricadevano nell'ambito di applicazione degli artt. 18-22 del Codice, che stabilivano le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.)*." Pertanto, in considerazione della sua natura di ente pubblico non economico, l'OPI è obbligato alla designazione di un DPO.

Inoltre, ai sensi del paragrafo 5 del suddetto art. 37 GDPR, "*il Responsabile per la Protezione dei dati (di seguito anche DPO) è designato 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*".

Si precisa che secondo l'art. 37, paragrafo 6, il DPO può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Inoltre, per essere in linea con le previsioni normative di cui all'art. 38 del GDPR, il DPO deve essere caratterizzato da:

- *autonomia* ed *indipendenza*, vale a dire che non deve esserci interferenza e istruzione ad opera di titolare o responsabile del trattamento rispetto alle attività ed alle funzioni aziendali che il DPO deve assolvere;
- *professionalità*, che equivale al possesso di comprovate e specifiche competenze in materia di privacy, necessarie per l'espletamento delle delicate funzioni ad esso attribuite;

- *continuità d'azione*, ovvero costanza nello svolgimento del proprio compito in ordine al rispetto del Regolamento UE 2016/679, del presente Sistema e delle procedure ad esso riferibili, nonché nell'assicurarne il periodico aggiornamento.

4.2. Requisiti

La nomina del DPO è subordinata:

- all'assenza di cause di incompatibilità e di motivi di conflitto di interesse con altre funzioni e/o incarichi che possano minarne l'indipendenza e la libertà di azione e di giudizio;
- alla dimostrazione di capacità professionali adeguate al ruolo da ricoprire, con particolare riguardo alla conoscenza della materia Privacy di cui al Regolamento UE 2016/679 e delle sue prassi applicative.

4.3. Nomina, durata e revoca

Il DPO è nominato dal titolare o responsabile del trattamento dell'Ordine delle Professioni Infermieristiche di Foggia.

Nell'ottica di garantirne la piena indipendenza ed autonomia di azione, il DPO riferisce, ai sensi dell'art. 38, paragrafo 3, GDPR, direttamente al Titolare del Trattamento o al Responsabile.

Il venir meno anche di uno solo dei requisiti di professionalità, assenza di incompatibilità e/o conflitto di interesse di cui al precedente paragrafo, in costanza di mandato, determina la decadenza dell'incarico.

La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento. In particolare, risultano con la stessa incompatibili:

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

4.4. Compiti del DPO

Nello svolgimento della sua attività, il DPO –sotto la sua diretta sorveglianza e responsabilità– può avvalersi, se necessario, del supporto di altre funzioni aziendali, ovvero di consulenti esterni, in quanto, in virtù dell'art. 38, paragrafo 2, GDPR, il titolare del trattamento e il responsabile del trattamento lo sostengono nell'esecuzione dei compiti di cui all'articolo 39 GDPR, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Ai sensi dell'art. 39 GDPR, al DPO sono conferiti almeno i seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Inoltre, nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto

conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il Titolare ed il Responsabile del trattamento forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

4.5. Poteri

Per lo svolgimento dei propri compiti, il DPO:

- gode di poteri ispettivi e di accesso ai documenti dell'Ente;
- dispone di risorse finanziarie e professionali adeguate;
- si avvale del supporto e della cooperazione delle varie strutture comunali, che possano essere interessate o comunque coinvolte nello svolgimento delle attività di controllo;
- può avvalersi di terzi esterni, portatori di competenze necessarie per l'ottimale svolgimento dei propri compiti.

Inoltre, il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

4.6. Funzionamento del DPO

Il DPO adotta un apposito regolamento interno disciplinante le modalità operative del proprio funzionamento (convocazioni, programma delle verifiche, piano della formazione, ecc.), adoperando le risorse finanziarie ed umane messe a disposizione dal titolare o responsabile del trattamento dei dati personali.

4.7. Flussi informativi verso il Titolare e il Responsabile del Trattamento

Il DPO può essere consultato in qualsiasi momento dall'Ente per riferire in merito al funzionamento del Sistema o a situazioni specifiche mentre, in

caso di particolari necessità, può informare direttamente e su propria iniziativa al vertice gerarchico del titolare o responsabile per il trattamento dei dati personali.

4.8. Flussi informativi verso il DPO

Ai sensi dell'art. 38, paragrafo 4, GDPR, gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento UE 2016/679.

Al DPO, inoltre, dovrà essere comunicata ogni informazione, di qualunque tipo, proveniente anche da terzi ed attinente all'attuazione del Sistema, nei termini e con le modalità che seguono.

Il DPO è l'Avv. Adamo Brunetti e potrà essere contattato mediante comunicazione scritta indirizzata al seguente indirizzo e-mail: a.brunetti@code4com.it

4.8.1. *Segnalazione delle violazioni che potrebbero comportare una responsabilità per l'Ordine delle Professioni Infermieristiche di Foggia*

I soggetti tenuti all'osservanza del Sistema di gestione dei trattamenti devono informare il proprio superiore gerarchico e/o il DPO di qualunque evento che potrebbe ingenerare in capo all'Ente una responsabilità amministrativa, in relazione a violazioni del Regolamento UE 2016/679, di legge o delle procedure previste dal presente Manuale.

Tale obbligo di informazione sussiste anche nei confronti dei collaboratori esterni dell'ente per espressa previsione contrattuale.

5. ADOZIONE DEL SISTEMA DI GESTIONE DEI TRATTAMENTI DA PARTE DELL'ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI FOGGIA

5.1. Obiettivi perseguiti con l'adozione del Sistema

OPI Foggia –nell'ottica di assicurare la protezione dei dati personali trattati nello svolgimento delle sue attività e di rispettare il GDPR – ha ritenuto doveroso, nell'ambito del rispetto dell'interesse pubblico connesso all'esercizio di pubblici poteri, implementare un sistema di gestione dei trattamenti nel rispetto delle previsioni normative di cui al Regolamento 2016/679.

Tale sistema è ispirato ai principi di correttezza, trasparenza, limitazione della finalità del trattamento, minimizzazione dei dati, esattezza dei dati, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

Nel contempo, esso rappresenta una linea guida per tutti coloro che operano nell'ambito o nell'interesse dell'OPI Foggia al fine di gestire i dati personali degli interessati in modo sicuro e conforme al GDPR ed alla normativa italiana in materia di Privacy.

5.2. La metodologia seguita nella costruzione del Sistema

La metodologia seguita nella predisposizione del sistema di gestione dei trattamenti ha avuto riguardo alle indicazioni fornite dalle *Linee Guida del GRUPPO DI LAVORO ARTICOLO 29 per la Protezione dei dati personali (in particolare WP 243 rev. 01 del 13 dicembre 2016, WP 248 rev. 01 del 4 ottobre 2017 e WP 253 del 3 ottobre 2017)*.

Il sistema così strutturato è stato articolato attraverso le seguenti fasi:

A. **MAPPATURA DEI TRATTAMENTI** dei dati personali in relazione ai singoli processi aziendali;
B. ***GAP ANALYSIS***, effettuata attraverso lo studio del sistema di gestione *privacy* esistente e che ha contemplato:

- l'esame dei documenti in materia di *privacy* già adottati dall'ente;
- le interviste con i responsabili di funzione;

- l'individuazione dei processi del Dipartimento Mobilità e Trasporti di Roma Capitale e dei relativi responsabili con riferimento alle attività di trattamento dei dati;
- la comparazione tra il sistema di gestione rilevato ed i *requirements* del Regolamento.

C. *PRIVACY IMPACT ASSESSMENT* che ha implicato l'analisi, condotta secondo i canoni del *risk management,* dell'impatto del trattamento dei dati sulle libertà e i diritti degli interessati.

Conseguentemente, il sistema è stato implementato mediante:

- la predisposizione del **Registro dei Trattamenti**;
- la delineazione delle **Procedure di gestione** dei trattamenti;
- la redazione delle **informative**;
- la redazione delle formule per la **manifestazione del consenso**;
- le **Nomine dei responsabili** del trattamento;
- le **Nomine dei designati** interni autorizzati ai trattamenti dei dati.

5.3. Funzione del Sistema

Scopo del presente documento è la predisposizione di un Sistema, strutturato ed organico, di procedure ed attività di controllo che sia funzionale all'esigenza di prevenire la commissione di quelle violazioni in materia di *privacy* previste dal Regolamento nell'ambito dello svolgimento delle attività tipiche dell'Ordine delle Professioni Infermieristiche di Foggia.

Ciò consente l'individuazione dei *trattamenti a rischio violazione* assicurando la possibilità di prevenire rischi nella gestione dei trattamenti dei dati personali.

5.4. Struttura del Sistema di gestione

Il presente sistema è composto dai seguenti documenti:

1. **Manuale – Doc. 1**, nel quale è descritto il Sistema di Gestione dei trattamenti ed è indicata la relativa metodologia di realizzazione; al manuale è altresì allegato l'Organigramma *Privacy*;
2. **Registro dei trattamenti – Doc. 2**, contenente l'insieme dei trattamenti effettuati per ogni processo aziendale;
3. **Valutazione di Impatto (DPIA) - Doc. 3**, in cui è riportata la stima del livello di rischio per i diritti e le libertà degli interessati connesso ai trattamenti, rispetto al quale sono state poi definite le misure tecniche ed organizzative idonee a gestirlo;
4. **Schemi delle Informative – Doc. 4** da impiegare per la comunicazione agli interessati delle finalità e delle modalità con cui sono realizzati i trattamenti da parte del titolare, ai sensi degli artt. 13-14 GDPR;
5. **Schemi delle Nomine – Doc. 5**, da utilizzare per la designazione dei soggetti autorizzati ai trattamenti e dei responsabili dei trattamenti ai sensi dell'art. 28 GDPR;
6. **Registro di accesso ai dati personali – Doc. 6**, nel quale potranno essere annotati gli accessi ai dati da parte degli interessati che ne hanno fatto richiesta;
7. **Procedure – Doc. 7**, all'interno delle quali vengono disciplinate concretamente le misure tecniche ed organizzative che l'ente dovrà porre in essere a garanzia della correttezza dei trattamenti di dati personali dalla stessa svolti. Nello specifico, sono state predisposte le seguenti procedure:
    - ***P_GDPR_01:*** Policy sul periodo di conservazione dei dati personali;
    - ***P_GDPR_02:*** Procedura di gestione dei dispositivi informatici;
    - ***P_GDPR_03:*** Procedura di gestione dei trattamenti in formato cartaceo;
    - ***P_GDPR_04:*** Procedura di gestione delle richieste degli interessati;

- ***P_GDPR_05:*** Procedura RAEE;
- ***P_GDPR_06:*** Procedura data breach;
- ***P_GDPR_07:*** Procedura di gestione della videosorveglianza

6. FORMAZIONE ED INFORMAZIONE

6.1. Formazione del dipendente di OPI Foggia

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della *privacy*, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l'ente sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, l'Ente riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con l'ente stesso.

Per garantire la conoscenza capillare delle disposizioni normative vigenti, l'Ente organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle

misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera OPI Foggia. La partecipazione del personale agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

6.2. Contenuti della formazione ed informazione

I contenuti formativi avranno ad oggetto tematiche afferenti le disposizioni normative in materia di *privacy*, i principi contenuti nel sistema di gestione e nelle procedure e regole di comportamento ad esso riferibili, nonché le specifiche finalità preventive che il sistema di gestione intende perseguire.

I moduli formativi sono articolati in relazione ai ruoli, alle funzioni e alle responsabilità rivestite dai singoli Destinatari nonché al livello di rischio del processo in cui gli stessi andranno applicati.

7. ANALISI DEI RISCHI

7.1. Premessa

La presente sezione rappresenta il documento di raccordo dell'attività di analisi e valutazione dei rischi compiuta da parte dell'Ordine delle Professioni Infermieristiche di Foggia per la redazione del Sistema di Gestione dei trattamenti ai sensi del Regolamento UE 2016/679.

In essa, dunque, vengono in maniera sintetica e conclusiva esplicati i trattamenti effettuati ed i risultati conseguiti nella fase preliminare alla definizione del sistema di prevenzione dei rischi di trattamento dei dati.

7.2. Attività di analisi dei rischi

L'analisi dei rischi si configura nel Regolamento UE 2016/679 come un'attività finalizzata al mantenimento della sicurezza e alla prevenzione dei trattamenti in violazione delle prescrizioni ivi dettate.

Rappresenta il primo ed imprescindibile passaggio nel percorso di definizione del Sistema di Gestione dei trattamenti *ex* Regolamento 2016/679, consentendo al Titolare:

- ✓ l'individuazione delle minacce attualmente presenti;
- ✓ l'individuazione, adozione ed aggiornamento nel tempo delle contromisure di sicurezza "*adeguate*";
- ✓ il riscontro alle richieste di esercizio dei diritti dell'interessato;
- ✓ la predisposizione di idonee informative *privacy* verso gli aventi diritto;
- ✓ la gestione della *governance privacy* interna ed esterna;
- ✓ la gestione degli obblighi relativi ai trasferimenti di dati all'estero.

Ciò posto, tale attività di analisi dei rischi va svolta sia per i trattamenti già in essere, che per i nuovi trattamenti posti in essere dal titolare avendo cura di provvedere ad una costante e puntuale mappatura degli stessi funzionale a garantire un adeguato livello di sicurezza e prevenire in modo tempestivo eventuali non conformità alla normativa.

Nello specifico, attraverso l'analisi del rischio (cfr. art. 32) viene effettuata una valutazione dei rischi connessi ai trattamenti e una valutazione degli impatti connessi alla protezione dei dati.

Al riguardo, per quanto concerne l'OPI Foggia, siffatta attività è stata condotta:

a) mediante un'analisi documentale;
b) attraverso interviste al fine di approfondire, appunto, la conoscenza dell'attività dei trattamenti;
c) tramite l'utilizzo della Tecnica FMEA (*Failure Mode and Effect Analysis*).

* * *

Le interviste sono state condotte dai consulenti di CO.DE S.r.l. al segretario dell'Ordine Delle Professioni Infermieristiche di Foggia, Dott. Matteo Vizzani.

In tale attività, nel corso dei colloqui è stato richiesto di indicare e descrivere le tipologie di trattamento caratterizzanti il processo o i processi (come responsabile o come consulente).

Inoltre, si è richiesto di offrire una valutazione circa:

a) la probabilità di violazione del trattamento dati;
b) l'impatto sui diritti delle persone e l'impatto economico reputazionale aziendale;
c) i rischi inerenti ai trattamenti dei dati;
d) l'adeguatezza delle misure per la limitazione di tali rischi.

7.3. *FMEA - Failure Mode and Effect Analysis*

Nel seguito verranno forniti strumenti di guida all'applicazione della *FMEA*, tecnica utilizzata per studiare e gestire il rischio.

La *FMEA* consente di effettuare un'analisi qualitativa di un sistema per determinare:

- ✓ i possibili **inconvenienti/minacce**[1] (c.d. ***failure mode***), cioè quello che potrebbe accadere qualora si verificasse una violazione delle informazioni;
- ✓ gli **effetti** (***effects***) di un inconveniente sulla stabilità dell'intero sistema.

Qualora all'analisi qualitativa *FMEA* si affianchi un'analisi quantitativa che consenta di classificare i *failure mode* in base ad un indice di priorità di rischio che permette di stabilire le priorità di intervento (c.d. rischi

[1] Minacce: sono entità (individui, eventi, ecc.) capaci di causare un danno.

prioritari), supportando l'assunzione di decisioni operative coerenti, si parla di *FMECA*.

Ad ogni modo, nell'uso comune, nel fare riferimento alla *FMEA* si intende la *FMECA*.

L'analisi condotta attraverso la *FMEA* consente di abbassare il rischio che si verifichino inconvenienti tali da determinare violazioni per effetto di operazioni e/o attività mal eseguite o non eseguite nell'ambito di ciascun processo.

In tal modo vengono prese in considerazione preventivamente tutte le possibili minacce all'interno del processo, permettendo di prevedere controlli, sviluppare procedure, predisporre contromisure per la gestione dei reclami.

7.3.1. Descrizione del modello FMEA

Di seguito di indicheranno i vari *step* attraverso cui trova applicazione la *FMEA* (*Figura 1*).

Figura 1

***Step* 1. Scelta del processo**

Sono stati presi in considerazione tutti i processi nel cui ambito possono essere effettuati dei trattamenti.

***Step* 2. Formazione del team di lavoro**

È stato costituito un *team* di lavoro FMEA al fine di disporre di soggetti esperti per i vari processi esaminati.

Il *team* è composto dai consulenti della CO.DE S.r.l.

***Step 3.* Analisi del processo**

Il team ha effettuato un approfondito studio -mediante analisi documentale e interviste ai responsabili di funzione- dei singoli processi aziendali individuando -in tal modo- tutti i possibili trattamenti.

***Step 4*. Identificazione dei potenziali rischi (*failure mode*)**

Tale fase ha consentito di identificare i potenziali inconvenienti che si possono verificare nello svolgimento delle singole attività, e quindi i potenziali rischi che si possono verificare nella realizzazione di ciascuna attività il cui verificarsi potrebbe cagionare danni agli utenti[2].

In tal caso l'approccio seguito nell'analisi condotta ha tenuto conto delle potenziali problematiche riscontrabili nell'ambito di ciascuna attività esaminata.

***Step 5.* Descrizione degli effetti e delle misure di controllo**

L'attività successiva consiste nel descrivere per ogni *failure mode*, le possibili conseguenze (c.d. *effects*), vale a dire i possibili danni che potrebbe subire l'utente in caso di accadimento dell'evento indesiderato, e le misure di controllo presenti (c.d. barriere) che permettono di intercettare/impedire l'evento (ad es., procedure, *check-list*, doppi controlli, sistemi di allarme, ed altro).

Anche in tal caso, l'approccio seguito è stato quello di valutare i potenziali danni verificabili all'utente così ripartiti:

- ✓ **danni diretti:** è il danno dovuto all'azione diretta della minaccia (ad es., in caso di rottura di un computer, è il danno materiale legato all'apparecchio in uno al danno immateriale legato alle informazioni contenute);
- ✓ **danni indiretti:** è il danno dovuto all'azione indiretta della minaccia (ad es., la perdita di profitto dovuta a inattività, la perdita di

[2] Per "utenti" si intendono gli stakeholders coinvolti nel processo oggetto dell'analisi di gestione del rischio.

competitività, i danni derivanti da cause legali o dalla perdita d'immagine, ecc.).

Per una computa valutazione del danno potenziale si dovranno considerare sempre entrambe tali tipologie.

Step* 6. Stimare la gravità, la probabilità e la rilevabilità dei *failure modes

Le fasi sopra descritte consentono l'analisi qualitativa della *FMEA*. Lo *step* successivo consente di procedere all'analisi quantitativa relativa alla *FMECA* che consente di valutare le criticità individuate secondo i criteri di:

- ✓ gravità;
- ✓ probabilità;
- ✓ rilevabilità.

L'analisi dei rischi in tal modo condotta, rispetta le indicazioni cristallizzate nelle linee guida del Garante Privacy (cfr. WP 248 - "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati*") e la metodologia seguita con la norma UNI ISO 31000:2010 relativa alla "*Gestione del rischio – Principi e linee guida*".

In tal modo il rischio viene valutato come l'incertezza sugli obiettivi, inteso come funzione di una probabilità (l'incertezza) e di un impatto (l'effetto).

Tale analisi è, d'altronde, conforme a quanto espressamente statuito dal Regolamento UE laddove all'art. 32 fa riferimento al "*rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".

L'analisi dei rischi richiede quindi una valutazione tanto probabilistica che di impatto.

Si tratta ovviamente, di una valutazione di stima in quanto l'analisi su possibili eventi del futuro implicano sempre un'aleatorietà non quantificabile.

Ad ogni inconveniente si attribuisce un valore numerico rispetto a ciascun criterio.

La **gravità/impatto "*G*"** indica il danno che può subire l'utente a seguito dell'inconveniente ed è stata calcolata prendendo in considerazione il maggior danno che può subire l'utente.

Al fine di stimare la gravità/impatto, si è tenuto conto che la stessa è la risultante della correlazione dei seguenti fattori:

a) **impatto sui diritti e le libertà delle persone (interessati)**, relativo alle conseguenze dannose sui diritti delle persone che possono derivare in caso di violazione del trattamento dei dati;
b) **impatto Economico – Reputazionale,** relativo alle conseguenze dannose, sia in termini economico-patrimoniali, che di immagine, potenzialmente derivanti in caso di violazione del trattamento dei dati.

Nell'ambito della sicurezza delle informazioni vi sono tre obiettivi di sicurezza afferenti ciascuno ad un aspetto diverso del fornire protezione alle informazioni:

1. mantenimento della riservatezza;
2. integrità;
3. disponibilità.

Di seguito verranno dettagliati tali aspetti.

La **ISO 27005 (*Information security risk management*)** è il principale riferimento per la gestione del rischio nell'ambito della sicurezza delle informazioni.

***Riservatezza (R)*:** significa proteggere le informazioni da eventuali accessi da parte di soggetti non autorizzati.

Integrità(I): fa riferimento all'autenticità dell'informazione, nel senso che tale informazione non sia alterata (modificata, cancellata, spostata) e che la sorgente dell'informazione sia autentica (perdita di consistenza rispetto alla versione "originale").

Disponibilità (D) fa riferimento all'accessibilità dell'informazione da parte degli utenti autorizzati qualora se ne ravvisi la necessità.

La **probabilità (*P*)** rappresenta la possibilità o frequenza con la quale l'inconveniente si può verificare e la stima è basata:

- su dati storici (i precedenti: ricorrenza nella storia dell'ente di eventi negativi riconducibili ad una violazione dei dati);
- sull'esperienza dei componenti del gruppo di lavoro;
- sulla frequenza con la quale vengono svolte le operazioni a rischio;
- sugli studi e ricerche note.

La **rilevabilità R** rappresenta, invece, la possibilità che il potenziale inconveniente possa essere individuato dalle misure di controllo messe in atto dall'organizzazione prima che si verifichi.
Solitamente vengono utilizzate **scale di valori da 1 a 10** e la stima della **maggiore gravità e probabilità di accadimento di un inconveniente corrisponde ai valori più elevati, mentre la stima di un'alta rilevabilità dello stesso è rappresentata dai valori più bassi delle scale**.

Di seguito vengono dettagliate le scale utilizzate (Tab. 1, 2, 3 e 4).

Scala di valutazione della GRAVITÀ			
Gravità dell'errore		**Criterio**	**Punteggio**
Bassa	Nessun danno	Riferimento alla tabella successiva in corrispondenza del liv. BASSO	1
			2
	Danni minimi		3
			4
Media	Danni moderati	Riferimento alla tabella successiva in corrispondenza del liv. MEDIO	5
			6
Alta	Danni significativi	Riferimento alla tabella successiva in corrispondenza del liv. ALTO	7
			8
Critica	Danni permanenti	Riferimento alla tabella successiva in corrispondenza del liv. CRITICO	9
			10

Tabella 1

Criterio di attribuzione della Gravità			
Livello	**Riservatezza**	**Integrità**	**Disponibilità**
Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici;	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione;	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione;

	- stigmatizzazione; - perdita di fiducia; - perdita economica.	- perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	- perdita di fiducia; - perdita economica.
Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di:

	interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	- perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.
Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli

	(p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.
Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatto	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di

	impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.

Tabella 2

Scala di valutazione della PROBABILITÀ		
Probabilità dell'errore	**Criterio**	**Punteggio**
Improbabile	Un inconveniente ogni 5-10 anni	1
		2
Remota	Un inconveniente ogni 3-5 anni	3
		4
Occasionale	Un inconveniente ogni 6 mesi/1 anno o alcune volte nel giro di due anni	5
		6
Probabile	Un inconveniente una o più volte al mese	7
		8
Frequente	Un inconveniente ogni giorno o meno	9
		10

Tabella 3

Scala di valutazione della RILEVABILITÀ		
Rilevabilità dell'errore	**Criterio**	**Punteggio**
Molto elevata	Molto elevata la probabilità di accorgersi dell'inconveniente; i sistemi di verifica e controllo quasi certamente rilevano l'inconveniente; controllo sistematicamente applicato senza rilevazione di inadeguatezze	1
		2
Alta	Alta probabilità che l'errore sia rilevato; verifiche e controlli molto probabilmente rilevano l'errore; controllo sistematicamente applicato e bassa probabilità di rilevazione di inadeguatezze	3
		4
Moderata	Moderata probabilità che l'errore sia rilevato; è verosimile che i controlli rileveranno l'errore; vengono rilevate mancanze al controllo, soprattutto di tipo formale (esempio: inesattezze nelle procedure relative)	5
		6
Bassa	Bassa probabilità di rilevare l'errore; verifiche e controlli difficilmente rileveranno l'errore;	7

	il controllo è applicato sporadicamente o in modo completamente inadeguato, non garantendone, quindi, l'efficacia	8
Remota	Remota probabilità di rilevare l'errore; verifiche e controlli non rilevano o non possono rilevare l'errore; il controllo non è previsto o è assente nella pratica	9
		10

Tabella 4

Step 7. Determinare il Livello di Rischio Privacy

A questo punto, per ciascun inconveniente relativo ad un determinato trattamento all'interno del singolo processo preso in considerazione, sarà possibile calcolare la criticità complessiva stabilendo l'Indice di priorità di rischio denominato **Livello di Rischio Privacy (LRP)** dato dal prodotto dei tre valori precedentemente determinati:

LRP = GxPxR.

Tramite scale di valori da 1 a 10, prese a riferimento, l'LRP potrà assumere valori da **1 a 1000**.

Individuando le maggiori criticità ossia le situazioni in cui l'**LRP** è più alto si evidenziano i momenti del processo che richiedono miglioramenti e quindi una o più priorità di intervento.

VALORE DI PROBABILITA' X GRAVITÀ X RILEVABILITÀ	INDICE DEL RISCHIO
1-200	BASSO
201-400	MEDIO
401-600	ALTO
> 600	CRITICO

Un **LRP** elevato indica che il potenziale inconveniente provoca gravi conseguenze, ha una elevata probabilità di verificarsi e ha scarse possibilità di essere rilevato prima che l'utente ne sia vittima.

Va rilevato che il percorso metodologico attraverso il quale si giunge a calcolare il LRP è caratterizzato da valutazioni soggettive dell'intervistato ma, allo stesso tempo, tale aspetto risulta mitigato dalla combinazione dei tre elementi sopra menzionati.

In tal modo, sarà possibile creare una lista delle priorità (c.d. *Priority List*) ordinando i *failure modes* in base alle priorità di intervento (cfr. LRP decrescenti).

Il criterio di **accettabilità del rischio** definito dal *team* tiene conto di inconvenienti con rischio accettabile che presentano un LRP inferiore al valore medio calcolato considerando i LRP relativi a tutti gli inconvenienti per ciascun trattamento dello specifico processo.

Appare evidente che le azioni di miglioramento riguarderanno dapprima gli eventi con un LPR più elevato per poi affrontare quelli con valori via via decrescenti fino ad arrivare al valore medio sopracitato.

***Step 8.* Individuare le possibili cause**

Si procede con la determinazione delle cause dei *failure modes* mediante una loro analisi.

Una minaccia da sola non può produrre alcun danno.

Affinché si verifichi un danno, la minaccia dovrà tenere in considerazione una vulnerabilità, ossia un punto debole del sistema.

La metodologia seguita terrà conto delle motivazioni sottese al verificarsi dell'inconveniente.

***Step* 9. Definire le azioni di miglioramento e gli indicatori di monitoraggio**

In considerazione delle cause rilevate, sarà possibile individuare le azioni da porre in essere per ridurre:

- ✓ la probabilità che i potenziali inconvenienti prioritari (quelli con il valore LRP più elevato) possano verificarsi;
- ✓ la gravità delle conseguenze qualora si verifichino.

Le attività che andranno implementate per attuare il miglioramento dovranno essere coerenti rispetto alle cause degli inconvenienti individuati.

Le azioni di miglioramento andranno a riguardare, pertanto, la componente umana, tecnica od organizzativa.

Dovranno essere definiti, pertanto:

- ✓ **i tempi di interventi;**
- ✓ **i responsabili;**
- ✓ **gli eventuali costi.**

L'obiettivo perseguito sarà -ad ogni modo- di ridurre gli indici di gravità, probabilità e rilevabilità.

***Step 10.* Valutazione dell'efficacia delle azioni intraprese**

L'ultima fase sarà quella relativa alla valutazione delle azioni intraprese al fine di verificare eventuali miglioramenti del sistema di sicurezza.
La verifica può essere effettuata:

1. rivalutando il processo dopo che sia trascorso un adeguato periodo di tempo mediante la tecnica *FMEA*;
2. basandosi su appropriati indicatori di processo (attuazione di progetti formativi, elaborazione di procedure, ecc.) e di esito (n. eventi indesiderati, livello di soddisfazione dei clienti, ecc.) precedentemente individuati.

7.3.2. Conclusioni

L'applicazione della tecnica *FMEA* coinvolge gli operatori in una elaborazione critica del processo migliorandone la conoscenza e introducendo preventivamente barriere di sicurezza.

Si ottiene, in tal modo, una diminuzione della frequenza degli inconvenienti.

Conseguentemente, e sulla scorta di quanto sopra esposto, va rilevato che il sistema *FMEA* dovrà essere costantemente aggiornato ed adeguato alle variazioni del sistema aziendale.

La procedura di gestione del rischio consente di considerare l'errore come fonte di apprendimento per evitare il ripetersi di quelle circostanze che hanno indotto al verificarsi di quell'errore.