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

MANUALE

Identificativo documento	Sistema di Gestione dei Trattamenti
Versione	01
Data Approvazione	
Redatto da	CO.DE S.r.l.
Verificato	
Approvato	A.U.

REVISIONI

Versione	Data	Contenuto
01		Aggiornamento

INDICE

1. IL REGOLAMENTO (UE) 2016/679

1.1 Il regime di applicabilità del Regolamento UE 2016/679

Il 25 maggio 2018 è divenuto effettivamente applicabile il nuovo Regolamento Generale dell'UE sulla protezione dei dati che ha sostituito la Direttiva sulla protezione dei dati del 1995. Adottato in risposta alla massiccia espansione del trattamento dei dati personali dall'introduzione della Direttiva del 1995 e allo sviluppo di tecnologie sempre più intrusive, il Regolamento prende le mosse dalla Direttiva e dalla giurisprudenza della Corte di Giustizia dell'Unione Europea (CGUE) ampliando significativamente la Direttiva e rafforzando consideravolmente l'attuale regime europeo di protezione dei dati.

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.

Il nuovo regolamento – destinato a trovare applicazione 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 obbiettivi 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.

1.2.1 Ambito di territorialità

Il Regolamento (cfr. considerando da 14 a 27 e art. 3) supera il criterio dello stabilimento trovando applicazione:

- al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione quando le attività di trattamento riguardano 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. Principio della *Privacy by design – art. 25 GDPR*

L'art. 25 GDPR "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita" al comma 1 stabilisce che "……..il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati……..".

Tale principio, 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. Principio della *Privacy by default*

Al comma 2, invece, è previsto che "……..Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento……."

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) – art. 35 GDPR</u>

L'art. 35 GDPR "Valutazione d'impatto sulla protezione dei dati" prevede che "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*"

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.

Il Titolare del trattamento, quando svolge una valutazione di impatto, deve interfacciarsi con il Responsabile della protezione dati personali, qualora sia nominato.
È altresì previsto che la valutazione di impatto è richiesta quando:

- vi sia una valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10;
- la sorveglianza sistematica su larga scale di una zona accessibile al pubblico.

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. <u>Notifica nell'ipotesi di violazione dei dati personali – art. 33 GDPR</u>

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. <u>Introduzione dei registri delle attività di trattamento – art. 30 GDPR</u>

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 – C. 32 GDPR

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].

1.1.1. 1.2.5 Informativa – art. 13 GDPR

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.

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 – C74 e art. 24 GDPR

Il titolare è definito all'art. 4 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.

2.2 Contitolare del trattamento – art. 26 GDPR

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 – art. 28 GDPR

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.

Per quanto concerne Errefin S.r.l., l'incarico di Responsabile del trattamento dei dati viene assegnato a qualunque soggetto esterno che esegue trattamenti di dati per conto della Società.

2.4 Destinatario - C31 GDPR

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.

Nel caso che 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 – art. 29 e C81 GDPR

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 – art. 37 GDPR

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 – art. 27 GDPR

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 – art. 51 GDPR

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

2.10 Comitato Europeo per la protezione dei dati – art. 68 GDPR

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 DI ERREFIN S.R.L.

3.1 La natura di Errefin S.r.l. e le sue attività

Errefin S.r.l. è un'agenzia in attività finanziaria iscritta all'OAM al numero A6755, con mandato diretto Fides S.p.A. Gruppo Banco Desio.

La Società di occupa di cessione del quinto, prestiti ai pensionati e delegazione di pagamento, quest'ultima principalmente rivolta ai lavoratori dipendenti.

3.2 Struttura organizzativa

La struttura direzionale ed operativa di Errefin S.r.l. è costituita da una sede legale e amministrativa sita in Foggia, alla via San Lazzaro n. 35-37.

Il sistema Privacy della Società è caratterizzato dalle seguenti figure:

a) titolare dei trattamenti;

b) responsabili dei trattamenti;

c) designati;

d) soggetti interessati.

Il sistema di *governance privacy* di Errefin S.r.l. è illustrato nell'organigramma della Società allegato al presente documento (**ALL. n.1**), nel quale sono rappresentate le diverse funzioni responsabili che caratterizzano la struttura operativa.

4. ADOZIONE DEL SISTEMA DI GESTIONE DEI TRATTAMENTI DA PARTE DI ERREFIN S.R.L.

4.1 Obiettivi perseguiti con l'adozione del Sistema

La Società – nell'ottica di assicurare la protezione dei dati personali trattati – ha ritenuto doveroso, nel rispetto delle politiche aziendali adottate, implementare un sistema di gestione dei trattamenti nel rispetto delle previsioni normative di cui al Regolamento.

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 di *Errefin S.r.l.* al fine di prevenire il rischio di violazioni in materia di privacy.

4.2 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 dalla Società;

- le interviste con i responsabili di funzione;
- l'individuazione dei processi della Società 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.

4.3 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 della Società.

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

4.4 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, indicandone la metodologia di realizzazione e l'organigramma *privacy*;
2. **registro dei trattamenti – Doc. 2,** contenente l'insieme dei trattamenti effettuati per ogni processo aziendale;

3. **DPIA - Doc. 3**, relativo alla valutazione di impatto sulla protezione dei dati consentendo la stima del livello di rischio mediante la determinazione delle misure idonee a gestirlo;
4. **informative – Doc. 4** indispensabili per la validità del consenso.
5. **nomine – Doc. 5;**
6. **registro di accesso ai dati personali – Doc. 6;**
7. **procedure – Doc. 7**.

5. FORMAZIONE ED INFORMAZIONE

5.1 Formazione del personale

La Società promuove la conoscenza del Sistema di Gestione dei trattamenti e delle relative procedure tra gli organi apicali e i dipendenti.

Costoro, dunque, sono tenuti a conoscerne il contenuto, ad osservarlo ed a contribuire alla loro attuazione.

A tal fine il Titolare dei Trattamenti gestisce la formazione del personale articolata secondo le seguenti modalità:

1) personale responsabile di funzione e personale con funzioni di rappresentanza della Società:
    a) formazione al momento dell'attuazione del sistema di gestione e, successivamente, in occasione di modifiche e/o integrazioni;
    b) formazione al momento dell'assunzione dell'incarico;
    c) comunicazioni periodiche, anche attraverso e-mail, di aggiornamento;
    d) formazione periodica sulle novità normative;
2) altro personale:
    a) nota informativa interna al momento dell'approvazione del sistema e, successivamente, in occasione di modifiche e/o integrazioni;
    b) informativa in sede di assunzione per i neo assunti;
    c) comunicazioni di aggiornamento.

5.2 Informativa a collaboratori e *partner*

Errefin S.r.l. promuove la conoscenza e l'osservanza del Sistema anche tra i *partners*, i consulenti, i collaboratori, i clienti ed i fornitori.

A costoro verranno pertanto fornite apposite informative richiamanti i principi, le politiche e le procedure che la Società ha adottato in attuazione del sistema di gestione, nonché verranno predisposte delle apposite clausole contrattuali che verranno adottate dalla Società, e per le quali verrà richiesta espressa accettazione.

5.3 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.

6. ADOZIONE DEL SISTEMA DI GESTIONE DEI TRATTAMENTI DA PARTE DI ERREFIN S.R.L.

6.1 Premessa

La presente sezione rappresenta il documento di raccordo dell'attività di analisi e valutazione dei rischi compiuta da parte di *Errefin S.r.l.* 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.

6.2 Attività di analisi dei rischi aziendali

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 *Errefin S.r.l.*, 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 Titolare della Società.

In tale attività, nel corso dei colloqui è stato richiesto all'intervistato 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.

6.3 *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 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.

6.3.1 Descrizione del modello FMEA

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

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

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.

***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

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

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 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 della Società 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; - stigmatizzazione; - perdita di fiducia; - perdita	**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; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia;	**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; - perdita di fiducia; - perdita economica.

	economica.	- 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 interessati in termini di: - perdita di autonomia; - esclusione;	**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 degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà;	**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: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.

	- perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia; - perdita economica.	- 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 (p.e. sconvolgendola) 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 ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di	**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 interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - perdita di fiducia;

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

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

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; il controllo è applicato sporadicamente o in modo completamente inadeguato, non garantendone, quindi, l'efficacia	7
		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.

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.

6.3.2. 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.