D.P.I.A.

DATA PROTECTION IMPACT ASSESSMENT

Piano di Valutazione d'impatto sulla Privacy ai sensi dell'art. 35 Reg. 2016/679/UE

PARISE SRL CENTRO DI MEDICINA DEL LAVORO

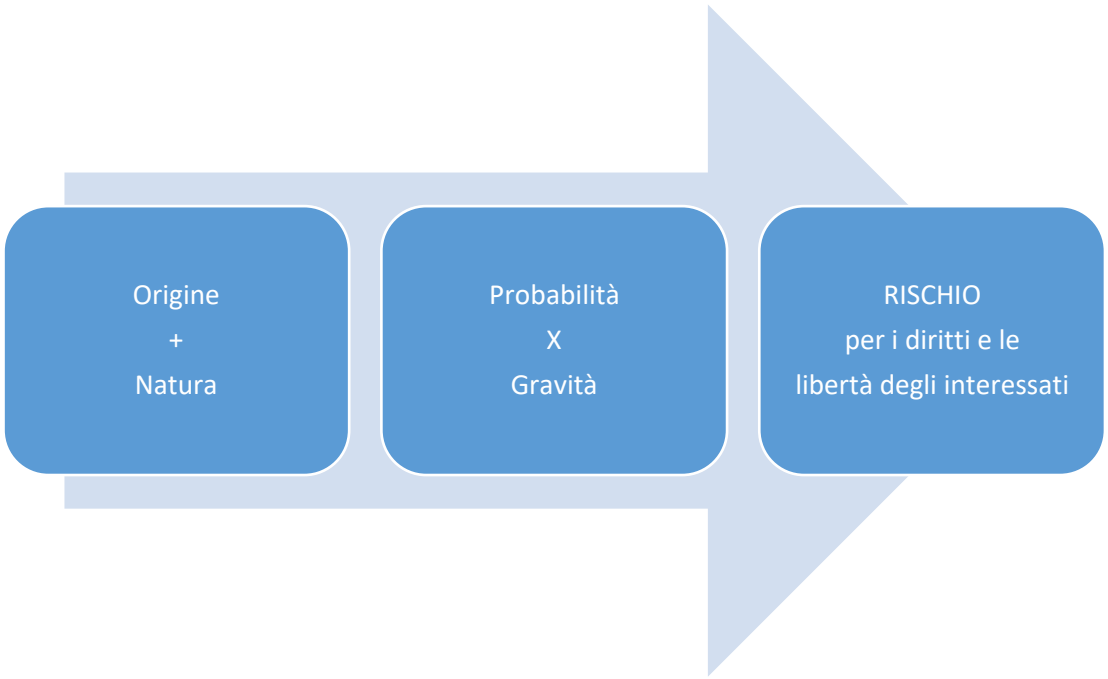
TRATTAMENTO DEI DATI PARTICOLARI NELLA SORVEGLIANZA SANITARIA

ALLEGATO AL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Autore: dott.ssa Cristina Froio
Validatore: dott. Riccardo Tacconi
Data: 30/03/2019

Version: 1.0

Sommario


Origine
+
Natura
Probabilità
X
Gravità
RISCHIO
per i diritti e le
libertà degli interessati

1	INTRODUZIONE: RAGIONI GIUSTIFICATRICI E SETTORE DI ATTIVITÀ

Il regolamento 2016/679/UE specifica "*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*".

Il trattamento soggetto a D.P.I.A. rientra fra le categorie generali indicate all'art. 35 par. 3 Reg. 2016/679/UE e riguarda:

- ☐ Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- ✓ **Trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;**
- ☐ Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il trattamento soggetto a D.P.I.A. rientra fra le categorie generali indicate all'art. 35 par. 4 Reg. 2016/679/UE, così come trasposte nel Provvedimento dell'Autorità Garante per la protezione dei dati personali n. 467 dell'11 ottobre 2018 "*elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*":

- ☐ Valutativi o di *scoring* su larga scala;
- ☐ Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" sull'interessato comprese le decisioni che impediscono l'esercizio di un diritto;
- ☐ Trattamenti che incidono "in modo analogo significativamente" sull'interessato, "ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi";
- ☐ Utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso APP, profilazione;
- ☐ Trattamenti su larga scala di dati aventi carattere estremamente personale, che fanno riferimento, fra gli altri, ai dati connessi alla vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale, tra questi i dati di geo localizzazione che potrebbero limitare il diritto di circolazione;
- ☐ Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geo localizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
- ☐ Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
- ☐ Uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuali;
- ☐ Scambio tra diversi titolari di dati su larga scala con modalità telematiche;
- ☐ Interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
- ✓ **Trattamenti di dati appartenenti alle cd. categorie particolari ai sensi dell'articolo 9 oppure di dati relativi a condanne penali e a reati di cui all'articolo 10 interconnessi con altri dati personali raccolti per finalità diverse;**
- ☐ Trattamenti di dati in maniera sistematica dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;
- ☐ Trattamenti di dati in maniera sistematica dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
- ✓ **Altri trattamenti valutati come necessari dal titolare del trattamento e/o dal D.P.O. incaricato**.

SETTORE DI ATTIVITÀ:

Il **d.lgs. 81/2008** in materia di tutela della salute e sicurezza negli ambienti di lavoro, prescrive l'obbligo della sorveglianza sanitaria dei lavoratori subordinati in casi specifici. Nei casi in cui risulti obbligatoria, il datore di lavoro è tenuto ad individuare il medico competente attenendosi, nella scelta, a specifici requisiti di tipo professionale indicati dalla normativa stessa.
Il medico competente stabilisce il programma di sorveglianza sanitaria ed epidemiologica e lo attua secondo criteri e protocolli basati sull'evidenza. Gli accertamenti preventivi sono orientati a constatare l'assenza di controindicazioni alla mansione specifica che il lavoratore deve svolgere. Lo scopo della sorveglianza sanitaria è quello di:

- valutare l'idoneità specifica al lavoro;
- scoprire in tempo utile anomalie cliniche o precliniche (diagnosi precoce);
- prevenire peggioramenti della salute del lavoratore (prevenzione secondaria);
- valutare l'efficacia delle misure preventive nel luogo di lavoro;
- rafforzare misure e comportamenti lavorativi corretti.

La sorveglianza sanitaria dovrà tener conto che l'esposizione ad alcuni agenti cancerogeni e/o mutageni può presentare un rischio molto elevato per alcune categorie di lavoratori che presentino: ipersuscettibilità genetica o acquisita (ad es. condizioni comportanti una facilitazione dell'assorbimento, difficoltà di metabolizzare o eliminare le sostanze estranee).
Il medico competente informa il lavoratore sui rischi e sulle misure di prevenzione, sull'importanza di sottoporsi ai tutti i controlli medici necessari e sull'influenza che le abitudini comportamentali extra lavorative (quali l'abitudine al fumo) possono avere sull'eventuale sviluppo di patologie. Inoltre il medico competente fornisce specifica informazione sull'opportunità di proseguire la sorveglianza sanitaria, allo scopo di ridurre eventuali rischi aggiuntivi e/o effetti negativi a lungo termine ai lavoratori esposti a cancerogeni e/o mutageni al momento in cui termina l'esposizione per cambio mansione e/o per cessazione del lavoro. Un protocollo di sorveglianza sanitaria adeguato per lavoratori esposti ad agenti cancerogeni e/o mutageni deve:

- prevedere accertamenti mirati al rischio specifico;
- essere in grado di evidenziare danni alla salute precoci e misurabili;
- possedere adeguate caratteristiche in termini di sensibilità.

La presente valutazione d'impatto analizza come la società Parise S.r.l., qualificata dal committente come responsabile del trattamento per l'esecuzione del servizio oggetto del contratto, valuti i rischi connessi al trattamento dei dati di salute dei lavoratori soggetti a visita medica e quali misure abbia adottato per ridurre i rischi presi in esame.

2	TIPOLOGIA DI DATI OGGETTO DEL TRATTAMENTO

La **società Parise S.r.l.** tratta in modo sistematico una quantità rilevante di dati personali e particolari dei lavoratori subordinati di clienti che in questo caso sono imprese e società soggette all'obbligo prescritto dal d.lgs. 81/2008.

I dati trattati sono di natura personale ma soprattutto particolare, così come definiti dall'art. 9 G.D.P.R., dati idonei a "rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

Nello specifico sono trattati **dati personali** quali: nome, cognome, data e luogo di nascita, C.F., ruolo e mansione aziendale. Al fine di poter svolgere il proprio servizio lo studio medico ha la necessità di dover associare a questi dati personali anche **dati di salute** forniti direttamente dall'interessato o rilevati tramite visita. La sintesi dei dati trattati si trova nella cartella sanitarie e di rischio; a titolo esemplificativo si trattano eventuali situazioni di disabilità, patologie pregresse o sorte di recente, stato psico – fisico e, in generale, risultati della sorveglianza sanitaria inerente alle mansioni specifiche e alle attività lavorative svolte. Il medico può rilevare stati di salute collegati all'uso di sostanze tossicologiche e o all'uso di alcol nei casi prescritti per legge in funzione della tutela stessa del lavoratore e di terzi nell'esecuzione della mansione. Le principali finalità per cui tali dati sono trattati riguardano:

1. Redazione di relazioni di Sopralluogo a cura del Medico Competente ai sensi D.lgs. 81/08;
2. esecuzione degli accertamenti sanitari previsti dal protocollo sanitario stabilito dal Medico Competente, in base alle mansioni e ai fattori di rischio specifici;
3. esecuzione di accertamenti sanitari richiesti dal Medico Competente ad integrazione del protocollo sanitario;
4. adempimento delle procedure medico legali per la gestione Malattie Professionali (coordinamento in particolare con Inail, Ispettorato del Lavoro) di Dimissione o di eventuale positività agli accertamenti relativi allo stato di Tossicodipendenza (coordinamento in particolare con Sert);
5. visione e/o integrazione di Documenti di Valutazione del Rischio D.lgs. 81/08 e relativi allegati tecnici di approfondimento;
6. servizi di formazione e informazione D.lgs. 81/08.

3 PRINCIPI FONDAMENTALI DEL TRATTAMENTO

I dati raccolti sono **necessari** al fine di conseguire l'idoneità alla mansione specifica; viene rispettato il principio di **minimizzazione**, in quanto non vengono raccolti dati di salute diversi da quelli necessari, ciò è facilitato dall'individuazione dei rischi nel D.V.R. e dall'individuazione delle mansioni specifiche dei singoli lavoratori cui sono presenti rischi per le malattie professionali tabellate.

Le misure adottate dalla società Parise S.r.l. permettono di rispettare anche gli altri principi a corollario del trattamento tra *accountability, privacy by design e privacy by default*; in particolar modo la redazione del registro delle attività di trattamento, predisposto secondo le indicazioni di cui all'art. 30 G.D.P.R., permette di verificare in modo esaustivo la presenza dell'accountability.

Nelle tabelle sottostanti sono identificate le **basi giuridiche che rendono lecito,** il trattamento così come previsto dall'art. 6 G.D.P.R.:

	Tipologia di base giuridica del trattamento	Presente (specificato, se non presente "//")
A	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	**Non è base giuridica necessaria**; sono casi in cui il consenso non viene chiesto.
B	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso	**È base giuridica** che rende il trattamento lecito: il contratto di lavoro di tipo subordinato da cui si evince la necessità della sorveglianza sanitaria. I presupposti sono: la valutazione dei rischi da cui si prescriva come misura preventiva la visita ai propri lavoratori, e la nomina espressa in capo al Medico del Lavoro prescelto da parte del datore di lavoro. La nomina implica da parte del Committente (titolare dei dati dei lavoratori) l'accettazione della privacy e il trasferimento dei dati al Medico.
C	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	E' base giuridica valida per questo trattamento.
D	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	E' base giuridica valida per questo trattamento.
E	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Non è base giuridica valida per questo trattamento.
F	il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore	Il legittimo interesse del titolare del trattamento (datore di lavoro del lavoratore) consiste nella possibilità da parte dello stesso di far svolgere la mansione specifica al lavoratore e tutelare la salute e la sicurezza degli altri lavoratori.

Essendo dati di natura particolare vige, *in primis*, il divieto di trattamento posto dall'art. 9.1 G.D.P.R.; solamente la presenza di **presupposti legittimi** permette una deroga al paragrafo sopracitato.

	Trattamento dati particolari – art. 9.2 G.D.P.R.	**Presente**
a)	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al par. 1	Il consenso per questa attività specifica trattamento non è necessario.
b)	il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato	L'obbligo è provato dalla presenza di contratto di lavoro, dalle ragioni giustificatrici della sorveglianza sanitaria contenute del D.V.R. di ogni singola azienda.
c)	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso	Non è di rilievo nel caso specifico.
d)	il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato	Non è di rilievo nel caso specifico.
e)	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato	Non è di rilievo nel caso specifico.
f)	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali	Non è di rilievo nel caso specifico.
g)	il trattamento è 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	Non è di rilievo nel caso specifico.
h)	il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi,	La finalità è la medicina del lavoro; la mancanza della richiesta di consenso è giustificata da questa deroga e

	assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3	dall'Autorizzazione 1/2016 del Garante per la protezione dei dati personali.
i)	il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale	Non è di rilievo nel caso specifico.
j)	il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato	Non è di rilievo nel caso specifico.

4	DESCRIZIONE DEI DATI PRESI IN CONSIDERAZIONE

La presente valutazione d'impatto è focalizzata sul trattamento da parte di Parise S.r.l. dei dati di salute dei lavoratori. Il dato personale legato alla salute è compreso nel novero dei dati particolari, dati comprensivi di una sfera così intima della persona da rendersi necessario, nel trattarli, una particolare considerazione ed una particolare sfera di protezione. I dati di salute comprendono una categoria in cui sono presenti condizioni patologiche dell'individuo cui è possibile parlare "fittiziamente" di dati personali ultra sensibili. La protezione di questi dati è talmente importante che già il previgente Codice privacy (d.lgs. 196/03) prescriveva, e ancor oggi il Reg. 2016/679/UE prescrive che il loro trattamento sia consentito solo se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso a questi dati è di **rango almeno pari** ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile. In sintesi significa che ogni volta che qualcuno (persona fisica o giuridica, pubblica o privata) chiede l'accesso a questa particolare tipologia di dati, deve dimostrare di avere un interesse più che fondato, meritevole di tutela almeno quanto l'informazione cui intende accedere.

L'accertamento da parte del datore di lavoro dell'assenza di patologie che possano compromettere la salute del lavoratore è un interesse fondato su un principio, tutela della salute stessa oltre al mantenimento degli standard qualitativi della vita, consistenti nel non provocare o contribuire a causare malattie professionali, che è da inserire su un piano almeno parificato, se non addirittura su un piano superiore, rispetto alla tutela della riservatezza in via esclusiva della dignità del lavoratore. Nel porre l'attenzione su questa contrapposizione, va comunque precisato che la visita del medico competente non permette, in alcun caso, un conferimento di merito con il datore di lavoro sulle patologie che inficiano lo stato di salute; al più la discussione sarà focalizzata sulla presenza o meno dell'idoneità piena allo svolgimento della mansione. Per garantire la tutela dei dati particolari dei lavoratori, il Medico del lavoro attua delle procedure di archiviazione e conservazione dei dati presso la propria sede, e informa i datori di lavoro sulle modalità per il corretto trattamento dei dati (es. sigillo, identificazione di aree dedicate alle conservazioni inaccessibili a personale non incaricato, divieto di apertura della cartella sanitaria ecc).

5	DESCRIZIONE DEL PROCEDURE MESSE IN ATTO

Il responsabile del trattamento adotta una serie di misure, tra cui un protocollo sanitario, al fine di poter dettare le procedure necessarie a tutti i medici che effettuano la sorveglianza sanitaria. Le misure inserite sono necessarie per poter garantire uno standard di sicurezza oltre che comportamentale in quanto la quantità di dati trattati è notevole.

A tale proposito le misure messe in pratica sono:

- il cliente deve restituire sottoscritte le misure indicate dal protocollo (cui sono comprese le indicazioni sulla nomina del medico, informative sul trattamento dei dati e documenti contrattuali;
- invio dell'elenco dipendenti del cliente da sottoporre a sorveglianza sanitaria con relativa indicazione delle mansioni;
- effettuazione della visita da parte del medico come previsto dal protocollo sanitario, vengono raccolte anamnesi e dati sanitari che vengono gestiti nel massimo rispetto della privacy nel gestionale aziendale;
- i dati raccolti nelle cartelle sanitarie di aziende con più di 15 dipendenti vengono inviati in azienda in buste chiuse sigillate da conservarsi in luogo sicuro; per le aziende con meno di 15 dipendenti le cartelle sono conservate presso Parise S.r.l.;
- divieto assoluto per tutti i delegati da inoltrare a mezzo mail dati di natura particolare;
- tutti gli archivi informatici sono protetti da password; gli archivi cartacei sono conservati in appositi armadietti sorvegliati;
- è stato acquistato un gestionale in costante aggiornamento dal punto di vista della sicurezza informatica.

6	CATEORIE DI RISCHI PRESI IN ESAME

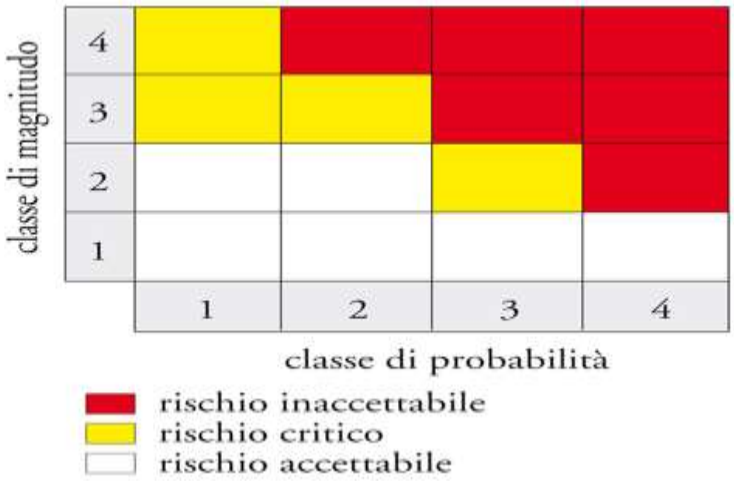
Nella presente sezione andranno valutati e stimati i rischi a seconda delle casistiche. È possibile sintetizzare e analizzare una violazione di sicurezza, come quella situazione che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati. Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).
Per semplicità è possibile riassumere le casistiche sopra indicate in tre macro categorie secondo la tipologia cd. **R.I.D.**:
R: Violazione di riservatezza (divulgazione o accesso a dati personali non autorizzato o accidentale);
I: Violazione di integrità (alterazione di dati personali non autorizzata o accidentale);
D: Violazione di disponibilità (perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali).
Sarà così possibile analizzare le cause e le conseguenze stimandone la gravità e la probabilità al fine di valutare se il grado e poter introdurre misure di sicurezza adeguate.

Il concetto della valutazione degli impatti, come previsto dall'art. 35 G.D.P.R., parte dal presupposto che il titolare del trattamento, o il responsabile del trattamento, abbia valutato che uno o più specifici trattamenti possano (per le modalità di svolgimento oppure per la particolarità dei dati trattai o ancora per l'utilizzo di strumenti tecnologici di ultima generazione) presentare un rischio grave per i diritti e libertà dell'interessato. Il punto di partenza dev'essere il principio dell'*accountability*, tramite il quale, il titolare possa dimostrare un ragionamento logico – giuridico che gli consenta di definire un trattamento di per sé rischioso; solo la mappatura specifica dei trattamenti e delle finalità, potrà definire la necessità della specifica e singola valutazione. Questa mappatura dovrà necessariamente arrivare dall'adozione del Registro delle attività di trattamento previsto dall'art. 30 G.D.P.R.

La valutazione d'impatto andrà comunque eseguita tramite presupposti di calcolo in termini di **probabilità x danno**, cui il titolare del trattamento deve identificare le ipotesi dannose (in termini di R.I.D.) e specificare quali misure ha adottato al fine di limitare, se non eliminare, quel particolare rischio.

Nella tabella sottostante sono presenti le indicazioni necessarie per poter leggere le considerazioni in termini di rischio prese in esame nelle casistiche riportate nel successivo paragrafo.

CLASSIFICAZIONE E MATRICE DI RISCHIO		
Nullo/trascurabile/basso	***Medio***	***Alto***
L'evento non causerebbe sottrazione//perdita irreversibile dei dati//sono stati sottratti i dati ma sono crittografati o comunque inutilizzabili, i dati sono anonimi e/o pseudonimi e quindi non è identificabile la persona; I dati sono di natura particolare ma non sono utilizzabili in quanto sono state prese misure di protezione idonee; il titolare/responsabile del trattamento ha posto misure preventive importanti per evitare il crearsi dell'evento La probabilità che si verifichi l'evento ipotizzato, nonostante la gravità non sia trascurabile, è molto limitata.	C'è stata sottrazione dei dati ma questi sono minimi o non compromettono in modo irreversibile l'interesse della persona. A titolo esemplificativo indirizzi e-mail e/o nomi di persone senza altri dati identificativi, e/o particolari; distruzione parziale di data base che comprometta l'esercizio dei diritti degli interessati.	sono stati sottratti dati personali e particolari/giudiziari oppure credenziali per l'accesso a conti correnti e/o posizioni personali, distruzione di banche dati non più recuperabili che compromettano in maniera definitiva l'esercizio dei diritti degli interessati; sono conosciuti dati particolari e utilizzati per finalità illecite oppure illegittimamente per altre finalità senza il rispetto dei diritti dell'interessato.



RISCHIO ANALIZZATO: RISCHIO REPUTAZIONALE

a. Principali minacce che potrebbero concretizzare il rischio

Inserire i potenziali rischi.

Danno esistenziale e danno morale causato al lavoratore per la divulgazione di dati da segretare.

b. Fonti di rischio prese in considerazione

Inserire le fonti di rischio: fonti umane interne, fonti umane esterne, fonti non umane (vedi definizioni).

Dolo del responsabile (Parise Srl): volontà di un proprio delegato di divulgare i dati (rischio residuale);

Errore del responsabile (Parise Srl): sua imprudenza negligenza imperizia comportamentale o informatica da cui ne deriva la divulgazione;

Dolo del cliente (potenzialmente coobbligato): volontà Sua o di un proprio delegato di divulgare i dati (rischio residuale);

Errore del cliente (potenzialmente coobbligato): Sua imprudenza negligenza imperizia comportamentale o informatica o di archiviazione da cui ne deriva la divulgazione;

c. Misure che contribuiscono a gestire il rischio

- ✓ Presenza di medici istruiti formati ed informati sulle responsabilità;
- ✓ Procedure fornite ai medici su come garantire la privacy degli interessati durante le visite;
- ✓ Presenza di personale autorizzato a trattare i dati, formato ed informato sui rischi;
- ✓ Presenza di strumenti idonei a conservare i documenti;
- ✓ Informazioni ai clienti in merito alla conservazione documentale lasciata in custodia presso il cliente stesso a tutela della dignità del lavoratore;
- ✓ Manutenzione ordinaria e straordinaria sui sistemi informatici.

Stima della **GRAVITÀ**: potenziali impatti (considerando anche i controlli pianificati).

Giustificare qui la gravità stimata del rischio, indicandone il relativo grado. Severità: rappresenta l'entità del rischio. Dipende principalmente dalla natura pregiudiziale del potenziale impatto.

- **Gravità trascurabile**: le persone interessate non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.
- **Gravità limitata**: le persone interessate potrebbero essere impattate da inconvenienti significativi ma che saranno in grado di superare nonostante alcune difficoltà.
- ✓ **Gravità significativa**: Le persone interessate potrebbero avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
- **Gravità massima**: Le persone interessate potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

Stima della **PROBABILITÀ**: tenendo in considerazione le minacce, fonti di rischio e i controlli pianificati).

Giustificare la probabilità stimata. La probabilità esprime la possibilità che un rischio si realizzi. Dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dal livello di capacità delle fonti di rischio a sfruttarle.

- ✓ **Probabilità trascurabile**: Basandosi sugli *asset* organizzativi non sembra possibile che le fonti di rischio considerate possano creare una minaccia.

- **Probabilità limitata**: Basandosi sugli *asset* organizzativi sembra difficile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità significativa**: Basandosi sugli *asset* organizzativi sembra possibile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità massima**: Basandosi sugli *asset* organizzativi sembra estremamente facile che le fonti di rischio considerate possano creare una minaccia.

Valutazione finale del rischio considerato: **basso, accettabile**

RISCHIO ANALIZZATO: USO DI DATI PER FINI DISCRIMINATORI

a. Principali minacce che potrebbero concretizzare il rischio

Inserire i potenziali rischi.

Conoscenza di patologie e/o situazioni relative all'interessato che, se messe nella disponibilità di datori di lavoro e/o colleghi potrebbero discriminare il lavoratore.

b. Fonti di rischio prese in considerazione

Inserire le fonti di rischio: fonti umane interne, fonti umane esterne, fonti non umane (vedi definizioni).

Dolo umano: volontà di conoscere e/o rendere conoscibili le informazioni;
Errore umano: imprudenza negligenza imperizia che comporta la conoscenza delle informazioni;
Problema tecnico: rottura dispositivi di conservazione delle informazioni;
Attacco informatico: divulgazione da parte di malintenzionati.

c. Misure che contribuiscono a gestire il rischio

- ✓ Presenza di medici istruiti formati ed informati sulle responsabilità;
- ✓ Procedure fornite ai medici su come garantire la privacy degli interessati durante le visite;
- ✓ Presenza di personale autorizzato a trattare i dati, formato ed informato sui rischi;
- ✓ Presenza di strumenti idonei a conservare i documenti;
- ✓ Informazioni ai clienti in merito alla conservazione documentale lasciata in custodia presso il cliente stesso a tutela della dignità del lavoratore;
- ✓ Manutenzione ordinaria e straordinaria sui sistemi informatici.

Stima della **GRAVITÀ**: potenziali impatti (considerando anche i controlli pianificati).

Giustificare qui la gravità stimata del rischio, indicandone il relativo grado. Severità: rappresenta l'entità del rischio. Dipende principalmente dalla natura pregiudiziale del potenziale impatto.

- **Gravità trascurabile:** le persone interessate non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.
- **Gravità limitata**: le persone interessate potrebbero essere impattate da inconvenienti significativi ma che saranno in grado di superare nonostante alcune difficoltà.
- **Gravità significativa**: Le persone interessate potrebbero avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
- ✓ **Gravità massima**: Le persone interessate potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

Stima della **PROBABILITÀ**: tenendo in considerazione le minacce, fonti di rischio e i controlli pianificati).

Giustificare la probabilità stimata. La probabilità esprime la possibilità che un rischio si realizzi. Dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dal livello di capacità delle fonti di rischio a sfruttarle.

- ✓ **Probabilità trascurabile**: Basandosi sugli *asset* organizzativi non sembra possibile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità limitata**: Basandosi sugli *asset* organizzativi sembra difficile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità significativa**: Basandosi sugli *asset* organizzativi sembra possibile che le fonti di rischio considerate possano creare una minaccia.

- **Probabilità massima**: Basandosi sugli *asset* organizzativi sembra estremamente facile che le fonti di rischio considerate possano creare una minaccia.

Valutazione finale del rischio considerato: **basso, accettabile.**

RISCHIO ANALIZZATO: TRATTAMENTO DELLE VISITE E DELLE CARTELLE SANITARIE

a. Principali minacce che potrebbero concretizzare il rischio

Inserire i potenziali rischi.

Mancato rispetto degli obblighi di legge che comporta la comunicazione o diffusione delle patologie o degli esami da cui si possono desumere stati di salute a chi non è autorizzato.

b. Fonti di rischio prese in considerazione

Inserire le fonti di rischio: fonti umane interne, fonti umane esterne, fonti non umane (vedi definizioni).

Imprudenza negligenza imperizia che comporta rischio elevato per conoscenza di dati sensibili riservati, causato da:

- archiviazione documentale non adeguata presso il medico o presso il cliente;
- archiviazione informatica non adeguata presso il medico o presso il cliente;
- mancato rispetto delle procedure comportamentali durante le visite;
- ambulatori di visita o aree di attesa che non rispettano la privacy (poca insonorizzazione, porte aperte, ecc..);

c. Misure che contribuiscono a gestire il rischio

- ✓ Ambiente di conservazione idoneo;
- ✓ Ambienti di visita idonei;
- ✓ Formazione e informazione del titolare del trattamento e suoi responsabili e delegati sulle responsabilità civili, penali e amministrative legate all'uso illecito;
- ✓ Nomine ai soggetti delegati alla conservazione;
- ✓ Informativa ai soggetti interessati attraverso cartellonistica e/o informativa specifica;
- ✓ Preparazione e rispetto di idonee procedure di conservazione.

Stima della **GRAVITÀ**: potenziali impatti (considerando anche i controlli pianificati).

Giustificare qui la gravità stimata del rischio, indicandone il relativo grado. Severità: rappresenta l'entità del rischio. Dipende principalmente dalla natura pregiudiziale del potenziale impatto.

- **Gravità trascurabile**: le persone interessate non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.
- **Gravità limitata**: le persone interessate potrebbero essere impattate da inconvenienti significativi ma che saranno in grado di superare nonostante alcune difficoltà.
- ✓ **Gravità significativa**: Le persone interessate potrebbero avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
- **Gravità massima**: Le persone interessate potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

Stima della **PROBABILITÀ**: tenendo in considerazione le minacce, fonti di rischio e i controlli pianificati).

Giustificare la probabilità stimata. La probabilità esprime la possibilità che un rischio si realizzi. Dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dal livello di capacità delle fonti di rischio a sfruttarle.

- **Probabilità trascurabile**: Basandosi sugli *asset* organizzativi non sembra possibile che le fonti di rischio considerate possano creare una minaccia.
- ✓ **Probabilità limitata**: Basandosi sugli *asset* organizzativi sembra difficile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità significativa**: Basandosi sugli *asset* organizzativi sembra possibile che le fonti di rischio considerate possano creare una minaccia.
- **Probabilità massima**: Basandosi sugli *asset* organizzativi sembra estremamente facile che le fonti di rischio considerate possano creare una minaccia.

Valutazione finale del rischio considerato: **basso, accettabile.**

7	PANORAMICA DEL RISCHIO E DEFINIZIONI

CONTROLLI DI SICUREZZA
Definizioni, controlli d'organizzazione, controlli di sicurezza funzionali, controlli di sicurezza fisici.

Crittografia

Misura che rende i dati personali incomprensibili a chiunque non abbia un'autorizzazione di accesso (crittografia simmetrica o asimmetrica, uso di algoritmi pubblici noti per essere robusti, certificato di autenticazione, ecc.). La crittografia di un messaggio garantisce che solo il mittente e il suo destinatario legittimo conoscano il contenuto del messaggio. Non avendo la chiave specifica il messaggio è inaccessibile e illeggibile, sia da esseri umani che da macchine. Ci sono due grandi famiglie di crittografia: simmetrica e asimmetrica.

- **crittografia simmetrica** per cifrare e decifrare il contenuto con la stessa chiave. È molto veloce ma richiede che il mittente e il destinatario concordino una chiave segreta comune o la scambino attraverso un altro canale, che deve essere scelto con attenzione per evitare che la chiave potrebbe essere recuperata dalle persone sbagliate, il che non garantirebbe più riservatezza del messaggio.
- **crittografia asimmetrica** suppone che il destinatario abbia una coppia di chiavi (chiave privata e pubblica) e fa in modo che il potenziale mittente abbia accesso alla sua chiave pubblica. In questo caso il mittente utilizza la chiave pubblica del destinatario per crittografare il messaggio, mentre il destinatario usa la sua chiave privata per decrittografarlo. Tra i suoi vantaggi c'è il fatto che la chiave pubblica può essere conosciuta da tutti e pubblicata. Ma attenzione: è necessario che i trasmettitori abbiano fiducia nell'origine della chiave pubblica, che siano sicure che sia effettivamente quella del destinatario. Un altro punto di forza: non è necessario condividere la stessa chiave.

Anonimizzazione

Processo di rimozione delle caratteristiche identificative dai dati personali. Per valutare la robustezza dei processi di anonimizzazione, consultare Linee guida WP29 .

Pseudonimizzazione

Trattamento dei dati personali in modo tale da non poter più essere attribuito a un interessato specifico senza l'uso di ulteriori informazioni, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a aspetti tecnici e organizzativi per garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile. La pseudonimizzazione riduce il rischio di correlazione di un set di dati con l'identità originale di un individuo, è un'utile misura di sicurezza, ma non un metodo di anonimizzazione.

Partizionamento dei dati

Metodi di organizzazione dei dati che riduce la possibilità che i dati personali siano correlati e che una compromissione di tutti i dati personali possa avvenire. Per esempio, possiamo identificare i dati specifici per ogni azienda separandoli logicamente.

Controllo degli accessi logici

Consiste nel limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale. Per fare ciò è consigliabile - definire i profili di autorizzazione nei sistemi separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine le loro missioni.

- rimuovere le autorizzazioni di accesso utente appena non dovranno più accedere a una risorsa locale o IT, nonché fine del contratto;
- realizzare una revisione annuale dei permessi per identificare ed eliminare gli account non utilizzati e riallineare i permessi concessi alle funzioni di ciascun utente.

Password

Le password devono essere composte da un minimo di otto caratteri, devono essere rinnovate periodicamente (*ogni sei mesi o una volta all'anno*) e ogni volta che c'è la minima preoccupazione che possano essere state compromesse e devono includere un minimo di tre o quattro tipi di caratteri (*lettere maiuscole, lettere minuscole, numeri e caratteri speciali*), quando una password viene modificata, le ultime cinque password non possono essere riutilizzate, la stessa password non deve essere utilizzata per accessi diversi; non deve essere correlata alle informazioni personali dell'utente(incluso nome o data di nascita). Definire un numero massimo di tentativi oltre i quali viene emesso un avviso e l'autenticazione è bloccata (temporaneamente o fino a quando non viene sbloccata manualmente).

Autenticazione

L'autenticazione è un'operazione con cui l'utente fornisce la prova dell'identità, per questo esistono diversi meccanismi classificati a seconda che coinvolgano:

- che cosa sappiamo, ad esempio una password;
- cosa abbiamo, ad esempio una smart card;
- una caratteristica della nostra persona, ad esempio un'impronta digitale o il modo di scrivere di una firma autografa.

Come promemoria il GDPR rende l'uso della biometria soggetto a autorizzazione preventiva da parte dell'autorità garante. L'autenticazione di un utente è qualificata come forte quando utilizza una combinazione di almeno due di queste categorie.

Sorveglianza

Configurare un'architettura di registrazione degli accessi e delle operazioni alle infrastrutture informatiche e fisiche per consentire l'individuazione precoce di incidenti che coinvolgono dati personali e disporre di informazioni che possono essere utilizzate per le analisi tecniche o per fornire prove in relazione alle indagini. In ogni caso, non conservare questi record per un periodo di tempo. eccessivo.

Archiviazione

Procedure che preservano e gestiscono gli archivi elettronici contenenti i dati personali destinati a garantire il loro valore (in particolare, il loro valore legale) per tutto il periodo necessario (trasferimento, archiviazione, migrazione, accessibilità, eliminazione, politica di archiviazione, protezione, ecc.). I dati che non vengono più utilizzati su base giornaliera ma non hanno ancora raggiunto il periodo di conservazione massimo, ad esempio perché conservato in caso di contezioso, devono essere archiviati. Gli archivi devono essere sicuri, soprattutto se i dati archiviati sono dati sensibili o che potrebbero avere gravi ripercussioni sugli interessati.

Filtraggio e rimozione

Quando i dati sono importati, diversi tipi di metadati (come EXIF allegati ad una immagine) possono essere collezionati involontariamente. Tali metadati devono essere identificati e eliminati se non sono necessari per gli scopi specificati.

Ridurre la sensibilità tramite conversione

Dopo aver ricevuto dati sensibili, come parte di un gruppo di informazioni generali o trasmessi solo a fini statistici, questi possono essere convertiti in un modulo meno sensibile o pseudonimizzato, ad esempio:

- se il sistema raccoglie l'indirizzo IP per determinare la posizione dell'utente a fini statistici, l'indirizzo IP può essere eliminato dopo aver detratto la città e il quartiere;
- se il sistema riceve dati video da telecamere di sorveglianza, e può riconoscere le persone in piedi o in movimento nella scena, sfocarle;
- se il sistema è un contatore intelligente, può aggregare l'uso di dati per un periodo di tempo, senza salvarli in tempo reale.

Gestione di progetto

Misure prese per integrare la protezione dei dati personali in nuove operazioni di trattamento (nomi fidati, linee guida, metodologia per la gestione del rischio o altre metodologie interne).

Compromissione dei dati personali

Compromissione della sicurezza che porta alla accidentale o illegittima distruzione, perdita, alterazione, pubblicazione o accesso non autorizzati di dati personali trasmessi, archiviati o altrimenti trattati.

Ridurre la natura identificativa dei dati

Il sistema può garantire che:

- l'utente possa utilizzare una risorsa o un servizio senza il rischio di rivelare la propria identità, dati anonimi);
- l'utente può utilizzare una risorsa o un servizio senza rivelare la sua identità, ma rimane identificabile e responsabile di tale utilizzo (dati pseudonimi);
- l'utente può fare molteplici utilizzi di risorse o servizi senza il rischio che questi usi possano essere collegati insieme (dati non correlati);
- l'utente può utilizzare una risorsa o un servizio senza il rischio che altri, in particolare terze parti, possano essere in grado di osservare che la risorsa o il servizio è in uso (non osservabilità. La scelta di un metodo dell'elenco di cui sopra dovrebbe dipendere dalle minacce identificate e, per alcuni tipi di minacce alla privacy, la pseudonimizzazione sarà più appropriata dell'anonimizzazione (ad esempio se c'è un bisogno di tracciabilità. Altre minacce alla privacy saranno affrontate con una combinazione di diversi metodi.

Ridurre l'accumulazione dei dati

Il sistema può essere strutturato in parti indipendenti con funzioni di controllo accessi separate, i dati possono anche essere distribuiti tra questi sottosistemi indipendenti e controllati da ciascun sottosistema utilizzando diversi meccanismi di controllo. Se un sottosistema compromesso, gli impatti sul set di dati possono essere ridotti.

Restrizioni d'accesso ai dati

Il sistema può limitare l'accesso ai dati in base a "*necessità di sapere*". Il sistema può cifrare i dati sensibili e applicare politiche di controllo degli accessi. Inoltre crittografare i dati sensibili per proteggerne la riservatezza durante la trasmissione e l'archiviazione. L'accesso ai file temporanei nascosti che vengono prodotti durante l'elaborazione dei dati deve essere protetto.

Fonti di rischio

Persona o fonte non umana che può causare rischio. Questa fonte può presentarsi accidentalmente o deliberatamente. Possono essere:

Fonti umane interne:

- un dipendente, malintenzionato, che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e il tempo di riserva potenzialmente disponibile o esser negligente a causa di un eventuale mancanza di formazione e consapevolezza.
- un utente o il suo entourage, incurante o malizioso, che ha accesso al servizio. Le sue motivazioni possono essere molteplici: imbarazzo, errore, negligenza, vendetta, volontà di allerta, malevolenza, possibilità di guadagno, spionaggio.

Fonti umane esterne:

- una terza parte malintenzionata o ignorante che utilizza la sua vicinanza fisica per accedere fraudolentemente al servizio;
- un utente malintenzionato che si rivolge a un utente utilizzando la sua conoscenza dell'utente e alcune informazioni su di esso;
- un utente malintenzionato che si rivolge a una delle società incaricata del trattamento utilizzando la sua conoscenza delle società che potrebbero consentire di attaccare la propria immagine;
- una terza parte autorizzata che utilizza il proprio accesso privilegiato per ottenere l'accesso non autorizzato alle informazioni. I motivi possono essere molteplici: gioco d'azzardo, molestia, malizia, vendetta, spionaggio, possibilità di profitto, acquisizione di dati per sfruttarli.

Fonti non umane:

- un incidente o un disastro in una delle organizzazioni incaricate del trattamento (*interruzioni di corrente, incendio, inondazione, etc*.).

Minaccia

Procedura comprendente una o più azioni individuali sulle risorse che supportano i dati. Agiscono, intenzionalmente o altrimenti, da fonti di rischio e possono causare un evento pericoloso.

8 DEFINIZIONE DELLE MISURE ADOTTATE E VALUTAZIONI CONCLUSIVE

La *ratio* per cui il G.D.P.R. prevede la redazione della valutazione d'impatto è strettamente connessa all'esigenza di responsabilizzare il titolare/responsabile del trattamento sui propri obblighi collegati alle finalità e modalità del trattamento. Potendo sintetizzare le questioni che queste figure si devono porre devono essere:

a) Il trattamento è strettamente necessario per le finalità?
b) In caso di risposta affermativa, le misure adottate in merito al trattamento specifico sono adeguate rispetto alle potenziali minacce e i relativi rischi ponderati?

I rischi precedentemente evidenziati (sezione 5) sono correlati alle attività di trattamento e non sono eliminabili. Di per sé, le stesse attività di trattamento si rendono necessarie per l'esecuzione, *in primis*, di un obbligo di legge (nello specifico la sorveglianza sanitaria come indicato dal d.lgs. 81/2008). Come affermato da tutte le leggi in materia che si sono susseguite nel corso degli anni, non è vietato il trattamento dei dati personali in generale, il presupposto però è che chiunque effettui attività di trattamento sia responsabilizzato sull'utilizzo mediante la predisposizione di misure tecnico ed organizzative che siano in grado di limitare il trattamento allo stretto necessario e che la figura dell'interessato sia completamente informata sia del trattamento specifico sia dei suoi diritti.

Il rischio (genericamente riassumibile con la formula **probabilità per danno**) è:

Basso: in quanto il responsabile incaricato adotta procedure atte a contenere i rischi sopra elencati con le misure riportate; nello specifico la società Parise S.r.l.:

SINTESI DELLE MISURE ADOTTATE A MITIGAZIONE DEL RISCHIO	
Redazione registro delle attività di trattamento secondo l'art. 30 G.D.P.R.	✓
Definizione di procedure generali a tutela dei dati raccolti	✓
Nomina del D.P.O. a garanzia delle misure adottate	✓
Protocollo predisposto da Parise S.r.l. messo a disposizione i documenti da firmare (contratto e nomina del medico)	✓
Ricezione elenco nominativi e mansioni in modo riservato con programmazione visite	✓
Effettuazione visite come previsto dal protocollo sanitario	✓
Invio cartelle sanitarie e di rischio all'azienda per la conservazione se l'azienda ha più di 15 dipendenti (contitolarità)	✓
Conservazione diretta delle cartelle sanitarie e di rischio all'azienda se l'azienda ha meno di 15 dipendenti	✓
Informazione ai pazienti sui loro diritti (diritti individuali)	✓
Nessun inoltro tramite mezzi non sicuri	✓