



“Il sistema di gestione della Protezione Dati: dal Registro delle attività di trattamento alla gestione dei Data Breach”

WEBINAR – 29 maggio 2019



Alberto Lombardi

*Resp. Protezione Dati - Resp. Ingegneria Clinica
ASL Benevento*

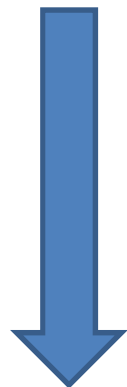
GUIDA ALL'APPLICAZIONE DEL
REGOLAMENTO EUROPEO
IN MATERIA DI PROTEZIONE
DEI DATI PERSONALI

EDIZIONE
AGGIORNATA
FEBBRAIO
2018



GDPR – Il nuovo approccio : Accountability e gestione del rischio

Art. 32: Il titolare deve adottare **opportune misure** e per **dimostrare** la conformità per quanto riguarda **l'individuazione del rischio** connesso al trattamento, la sua **valutazione** in termini di origine, natura, probabilità e gravità, e l'individuazione di **migliori prassi per attenuare il rischio**



INDICAZIONI DEL DPO

LINEE GUIDA DEL GARANTE e del WP

CODICI DI CONDOTTA
CERTIFICAZIONI



Dalla forma alla sostanza: Il nuovo approccio basato sul rischio

Art. 5.2: “Il titolare del trattamento è **competente** per il rispetto” dei principi applicabili al trattamento”.. **e in grado di provarlo**”

Cons. 74: (...il titolare del trattamento dovrebbe mettere in atto **misure adeguate ed efficaci ed essere in grado di dimostrare la conformità** delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure

Art. 24 - 1: «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, **nonché dei rischi aventi probabilità e gravità** diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative **adeguate per garantire, ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento.»



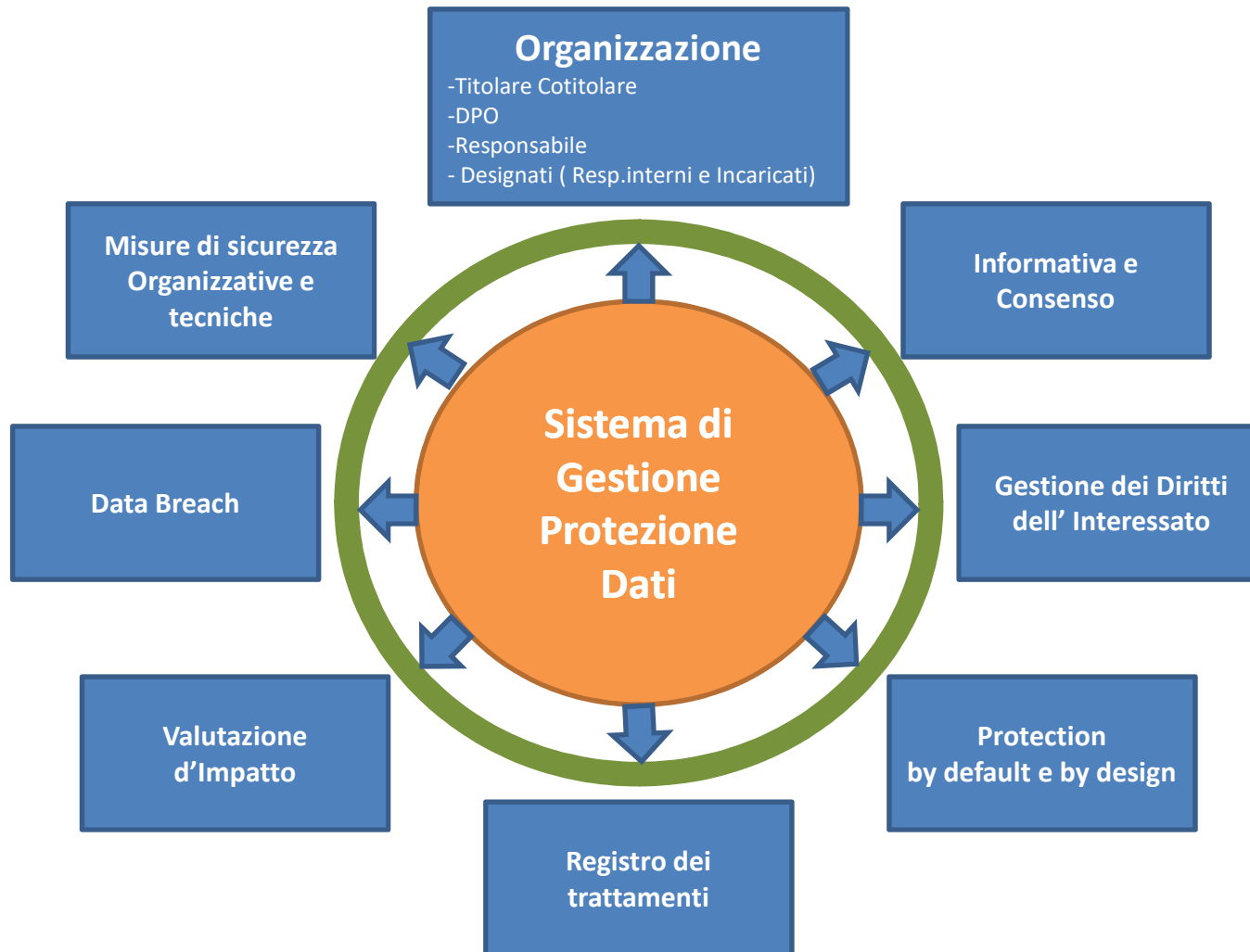
- **Conoscenza dei processi aziendali, dei flussi informativi e relativi trattamenti**
- **Individuazione, Valutazione e Gestione dei Rischi**
- **Adozione delle adeguate misure di sicurezza organizzative e tecniche**

Sistema di gestione e Organizzazione del lavoro

- Definizione di una **Strategia aziendale** condivisa di trattamento dei dati personali
- Implementazione di un **Sistema di Gestione della Protezione dei Dati** strutturato, per garantire una gestione efficace ed efficiente dei requisiti normativi in ottica di continuo miglioramento
- Individuazione di un **Programma di attuazione condiviso in materia di protezione dei dati personali**, suddiviso il processo in tre step principali:
 - **Assessment e mappatura** dei trattamenti, dell'organizzazione e delle procedure esistenti,
 - **Design e definizione nuovo modello** tecnico-organizzativo, con ridefinizione dei processi e delle metodologie di trattamento
 - **Management e Controllo del Sistema.**



Sistema di gestione e Organizzazione del lavoro



Registro delle Attività di Trattamento (art. 30 GDPR)

L'art. 30 del [Regolamento \(EU\) n. 679/2016](#) prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del [registro delle attività di trattamento](#).

E' un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento

[Costituisce uno dei principali elementi di accountability del titolare](#), in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante





Registro delle Attività di Trattamento (art. 30 GDPR)

L'obiettivo principale è permettere al Titolare del trattamento e ai suoi designati di avere conoscenza e consapevolezza di **“chi fa che cosa”**.

Senza un registro dettagliato, è difficile dimostrare di aver un controllo sul corretto trattamento dei dati personali, non è possibile illustrare i trattamenti nelle informative privacy, è difficile identificare i trattamenti che devono essere oggetto di valutazione d'impatto o DPIA

**CHI FA
CHE COSA**





Registro delle Attività di Trattamento – Chi deve redigerlo?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che **possano presentare un rischio – anche non elevato** – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che **effettui trattamenti non occasionali**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

Rientrano nella categoria delle “organizzazioni” di cui all’art. 30, par. 5 anche le associazioni, fondazioni e i comitati

Registro delle Attività di Trattamento (art. 30 GDPR)

L'obiettivo principale è permettere al Titolare del trattamento e ai suoi designati di avere conoscenza e consapevolezza di **“chi fa che cosa”**.

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso



Registro delle Attività di Trattamento (art. 30 GDPR)

| <i>Rif.</i> | <i>Attività prevista</i> |
|-------------|--|
| 1 | Ricostruzione del flusso di dati |
| 1.1 | Effettuare una rassegna completa del flusso dei dati in entrata, in uscita e all'interno dell'azienda. |
| 1.2 | Individuare tutti i dati personali detenuti dall'azienda, per ognuno individuando da dove il dato proviene, il tipo di dato e altri soggetti con le quali eventualmente il dato viene condiviso o trasmesso. |
| 1.3 | Individuare per ogni tipologia di dato le modalità di trattamento |



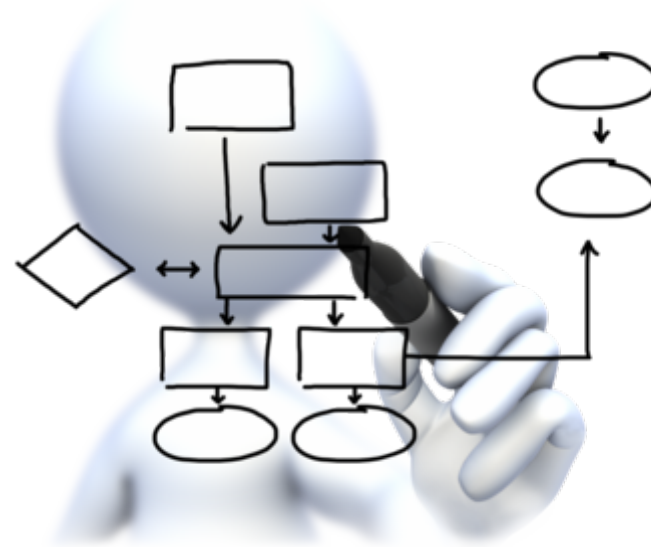
Mappatura dei processi e analisi dei flussi informativi

L'analisi ed individuazione dei trattamenti **deve essere** effettuata nella azienda attraverso un'attenta **mappatura dei processi** e quindi **analisi dei flussi informativi** ad esso sottesi

*Anche se i processi sono vitali per un'organizzazione perché sono il modo in cui essa realizza i suoi obiettivi e implementa le sue strategie, difficilmente **le aziende ne sono veramente consapevoli.***

*Manca **la consapevolezza di cosa si fa in azienda e di come lo si fa:** Le attività e le procedure sono spesso **nella mente delle persone.***

Questo porta con sé enormi rischi. Ad esempio il pensionamento di qualche figura cardine può provocare periodi di fermo o il rischio di ripartire con difficoltà dopo che si sono verificati problemi.



Mappatura dei processi e analisi dei flussi informativi

La mappatura dei processi e dei propri flussi informativi è composta dalle seguenti fasi fondamentali:

1. Identificazione delle **attività svolte**, e descrizione della situazione di “cosa avviene” nell’azienda.
2. Definizione, per ogni processo individuato, di **flussi informativi** e della **natura qualitativa e quantitativa dei dati trattati**.
3. Identificazione **e classificazione della tipologia di dati trattati**, in particolare l’identificazione di dati sensibili, ultrasensibili e giudiziari.
4. Identificazione e descrizione delle **modalità in cui il dato viene acquisito, elaborato, comunicato ed archiviato**.



Mappatura dei processi e analisi dei flussi informativi

5. Descrizione delle **articolazione aziendali**, delle **società esterne** o dei professionisti che **intervengono nel trattamento** con identificazione dei Responsabili esterni ed interni e di tutti gli attori che intervengono nel processo analizzato.

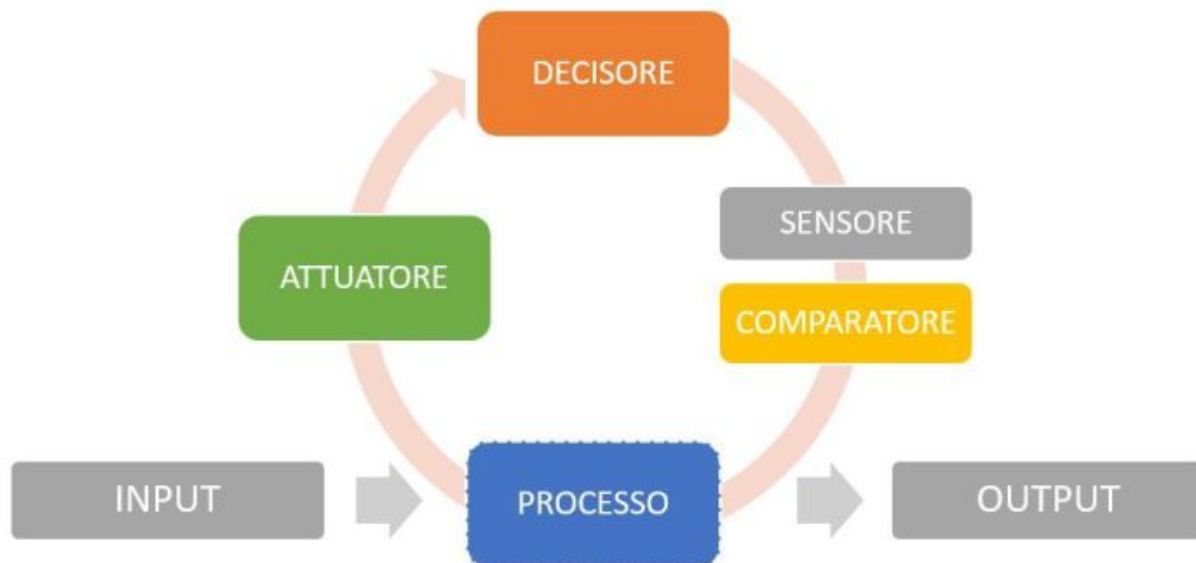
6. Identificazione dei **legami logici e delle interazioni con altri processi** e con ulteriori *attori* che intervengono nel trattamento a cui sono comunicati/trasmessi i dati.

7. **Semplificazione ed ottimizzazione dei processi**, cercando ridurre al minimo le informazioni utilizzate nel processo e il trattamento da effettuare sugli stessi (Protection by default e by design).



Mappatura dei processi e analisi dei flussi informativi

8. Individuazione e descrizione delle **misure organizzative e tecniche** utilizzate per garantire la sicurezza del trattamento con particolare riferimento alla trasmissione e all'archiviazione dei dati personali
9. Creazione di un **sistema in grado di monitorare i processi, i flussi informativi** e le tipologia di dati trattati al fine di apportare modifiche e miglioramenti ed adottare eventuali azioni correttive e preventive per garantire la sicurezza dei dati trattati.





Registro delle Attività di Trattamento

Quali informazioni deve contenere?

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del RGPD) e in quello del responsabile (art. 30, par. 2 del RGPD).

Con riferimento ai contenuti si rappresenta quanto segue:

(a) nel campo “**finalità del trattamento**” oltre alla indicazione delle stesse, distinta per tipologie di trattamento, sarebbe opportuno indicare anche **la base giuridica** dello stesso (v. art. 6 del RGPD; in merito, con particolare riferimento al “legittimo interesse”, si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le “garanzie adeguate” eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d’impatto posta in essere dal titolare)

Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno:

- in caso di trattamenti di “categorie particolari di dati”, indicare una delle condizioni di cui all’art. 9, RGPD;
- in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell’Unione europea) che ne autorizza il trattamento ai sensi dell’art. 10 del RGPD;

Quando il trattamento dei dati è lecito? (art. 6 del GDPR)





Trattamento lecito per categorie particolari di dati (art. 9 del GDPR)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Trattamento di dati sulla salute in ambito sanitario ai sensi del Regolamento (UE) 2016/679



Trattare «categorie particolari di dati» in ambito sanitario è sempre vietato, tranne che per:

- motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri
- motivi di interesse pubblico nel settore della sanità pubblica (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);
- finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura»)

I trattamenti che:

- sono essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute;
- e
- sono effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza

NON richiedono il consenso al trattamento dei dati da parte dell'interessato

E' possibile trattare dati sanitari SOLO con il consenso dell'interessato per:

- consultazione del Fascicolo sanitario elettronico
- consegna del referto online
- utilizzo di app mediche
- fidelizzazione della clientela
- finalità promozionali o commerciali
- finalità elettorali





Registro delle Attività di Trattamento

Quali informazioni deve contenere?

(b) nel campo “**descrizione delle categorie di interessati e delle categorie di dati personali**” andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

(c) nel campo “**categorie di destinatari a cui i dati sono stati o saranno comunicati**” andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. *enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi*). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. *soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento*). Ciò al fine di consentire al titolare medesimo di **avere effettiva contezza del numero e della tipologia dei soggetti esterni** cui sono affidate le operazioni di trattamento dei dati personali;



Registro delle Attività di Trattamento

Quali informazioni deve contenere?

(d) nel campo “**trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale**” andrà riportata l’informazione relativa ai suddetti trasferimenti unitamente all’indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle “garanzie” adottate ai sensi del capo V del RGPD;

(e) nel campo “**termini ultimi previsti per la cancellazione delle diverse categorie di dati**” dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (*ad es. “in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall’ultima registrazione – v. art. 2220 del codice civile”*). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. “in caso di contenzioso, i dati saranno cancellati al termine dello stesso”);



Registro delle Attività di Trattamento

Quali informazioni deve contenere?

(f) nel campo “**descrizione generale delle misure di sicurezza**” andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’art. 32 del RGDP tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere.

Tale lista ha di per sé un carattere dinamico (*e non più statico come è stato per l’Allegato B del d. lgs. 196/2003*) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi.

Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

Misure tecniche ed organizzative

Art. 32 GDPR





Registro delle Attività di Trattamento Può contenere informazioni ulteriori?

Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare ad es.:

- le modalità di raccolta del consenso
- la modalità di resa dell'informativa
- le modalità di gestione ed archiviazioni del trattamento
- i luoghi fisici del trattamento e quelli di archiviazione
- le eventuali valutazioni di impatto effettuate,
- l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento



Registro delle Attività di Trattamento

| | |
|--|--|
| UOC Riferimento | Tutti i Distretti |
| AREA riferimento | Dipendenze Patologiche |
| Nome Trattamento | Attività sanitarie correlate alle dipendenze |
| Descrizione sintetica del trattamento | Diagnosi e cura delle dipendenze patologiche e delle patologie associate |
| Titolare del trattamento | Direttore Generale ASL BN |
| Eventuale contitolare | |
| Responsabile interno trattamento | Direttore Distretto |
| Responsabile esterno trattamento | Gestore del SID (Sistema informatico Dipendenze) Gestore Winsimet (molteni) |
| Estremi contratto Responsabile esterno | |
| Descrizione Trattamento | Preso in carico del paziente con dipendenze patologiche, su base volontaria o segnalazione giudiziaria . Valutazione della patologia - trattamento terapeutico - termine trattamento. |
| Categoria interessati (scelta multipla) | Assabili |
| Natura dei dati (scelta multipla) | Identificati - Anagrafici, Sanitari e/o Ultrasensibili (Biometrici, etc), Giudiziari |
| Liceità del Trattamento (obbligo di legge, consenso, ...) | Consenso-Obbligo di Legge. L.309/90 |
| Finalità del trattamento | Assistenza su richiesta dell'utente o obbligo giuridico |
| Altre Strutture/Enti che concorrono al trattamento | tribunale, tribunale minori, U.E.P.E., Comunità terapeutiche, Prefettura. |
| Durata di conservazione dei dati | tempo illimitato |
| Modalità di raccolta dati (scelta multipla) | Automatizzata, Cartaceo, Digitale, Winsimet, SID |
| Modalità di archiviazione | Archivio Cartaceo, Archivio Digitale |
| Modalità di gestione del trattamento | Riconoscimento dell'utente con documento; processo di valutazione socio-sanitaria; compilazione di cartella clinica; effettuazione di esami tossicologici ed ematici per la valutazione medica. Archiviazione in locale parzialmente adibito ad archivio, inserimento sulla piattaforma SID e Winsimet per trattamento terapeutico |
| Modalità di resa dell'informativa | fornito modello cartaceo ASL |
| Modalità di raccolta del consenso al primo accesso | Tramite modello cartaceo ASL |
| Descrizione delle misure di sicurezza organizzative adottate nel trattamento | I locali del trattamento sono presidiati dagli incaricati dipendenti che chiudono la porta a chiave a fine orario lavorativo |
| Descrizione delle misure di sicurezza tecniche adottate nel trattamento | presenti armadi con chiusura a chiave e cassaforte con elenco degli isritti (per dati ultrasensibili); presenza di grate alle finestre e porta di ingresso con saracinesca |
| Procedura adottata per il trattamento | |
| Elenco degli incaricati coinvolti nel trattamento | Tutti gli operatori della UO incaricati al trattamento (vedi elenco specifico) |
| Luoghi fisici di trattamento dei dati | Locali della UO individuati in apposita scheda |
| Luoghi fisici della conservazione dei dati | Locali della UO individuati in apposita scheda |
| Trasferimento dati verso paesi terzi o organizzazioni internazionali | NO |

| | |
|---|---|
| ✓ | AREA riferimento |
| ✓ | Nome Trattamento |
| ✓ | Titolare del trattamento / contitolare |
| ✓ | Responsabile interno trattamento |
| ✓ | Responsabile esterno Estremi contratto |
| ✓ | Descrizione Trattamento |
| ✓ | Categoria interessati |
| ✓ | Natura dei dati |
| ✓ | Liceità del Trattamento (obbligo di legge, consenso, ...) |
| ✓ | Finalità del trattamento |
| ✓ | Altre Strutture/Enti che concorrono al trattamento |
| ✓ | Durata di conservazione dei dati |
| ✓ | Modalità di raccolta dati |
| ✓ | Modalità di archiviazione |
| ✓ | Modalità di gestione del trattamento / Procedure |
| ✓ | Modalità di resa dell'informativa |
| ✓ | Modalità di raccolta del consenso al primo accesso |
| ✓ | Descrizione delle misure di sicurezza organizzative |
| ✓ | Descrizione delle misure di sicurezza tecniche |
| ✓ | Elenco degli incaricati coinvolti nel trattamento |
| ✓ | Luoghi fisici di trattamento dei dati |
| ✓ | Luoghi fisici della conservazione dei dati |
| ✓ | Trasferimento dati verso paesi terzi o org internazionali |

Registro delle Attività di Trattamento

Quali sono le modalità di conservazione e di aggiornamento?

Il Registro dei trattamenti **deve essere mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere.

Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua **prima istituzione** (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella **dell'ultimo aggiornamento**. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

“- scheda creata in data XY”

“- ultimo aggiornamento avvenuto in data XY”





Registro delle Attività di Trattamento

Il registro del Responsabile

Il responsabile del trattamento tiene un registro di “tutte le categorie di attività relative al trattamento svolte per conto di un titolare” (art. 30, par. 2 del RGPD).

In merito alle modalità di compilazione dello stesso si rappresenta quanto segue:

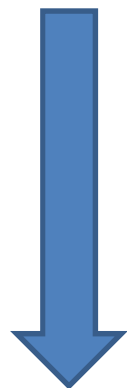
a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento **per conto di più clienti** quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all’art. 30, par. 2 del RGPD **dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari**. In questi casi il responsabile dovrà **suddividere il registro in tante sezioni quanti sono i titolari** per conto dei quali agisce; ove, a causa dell’ingente numero di titolari per cui si operi, l’attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall’art. 30, par. 2 del RGPD;

b) con riferimento alla “**descrizione delle categorie di trattamenti effettuati**” (art. 30, par. 2, lett. b) del RGPD) è possibile far riferimento **a quanto contenuto nel contratto di designazione a responsabile** che, ai sensi dell’art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest’ultimo;

c) in caso di sub-responsabile, parimenti, il registro delle attività di trattamento svolte da quest’ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell’art. 28, paragrafi 2 e 4 del RGPD.

GDPR – Il nuovo approccio : Accountability e gestione del rischio

Art. 32: Il titolare deve adottare **opportune misure** e per **dimostrare** la conformità per quanto riguarda **l'individuazione del rischio** connesso al trattamento, la sua **valutazione** in termini di origine, natura, probabilità e gravità, e l'individuazione di **migliori prassi per attenuare il rischio**



INDICAZIONI DEL DPO

LINEE GUIDA DEL GARANTE e del WP

CODICI DI CONDOTTA
CERTIFICAZIONI



GDPR – Il nuovo approccio : I rischi del trattamento dei dati

Il nuovo regolamento generale ha un approccio basato sulla **valutazione del rischio (risk based)**, piuttosto che sulla protezione dell'utente.

Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto **della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.**

Quindi, il rischio inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati.



GDPR – Il nuovo approccio : I rischi del trattamento dei dati

Un "**rischio**" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di **gravità** e **probabilità**

La "**gestione dei rischi**", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi





GDPR – Il nuovo approccio : I rischi del trattamento dei dati

Il Considerando 75 ci aiuta con riferimento al **concetto di rischio**:

*"I rischi per i diritti e le libertà delle persone fisiche, **aventi probabilità e gravità diverse**, possono derivare da trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale**, in particolare:*

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifrazione non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;*
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;*
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;*
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;*
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".*



GDPR – Il nuovo approccio : Tipologia di rischi - esempi

Trattamento (raccolta) di dati non necessario in base alla finalità - Vedi art. 5, par. 1 lett. b) (principio di finalità), art. 13

Informativa e termini non chiari o trasparenti - Vedi art. 4, par. 11 (consenso dell'interessato) e art. 13

Dati personali non aggiornati o **obsoleti** - Vedi art. 15 e 16 (diritto di rettifica)

Inefficace o intempestiva cancellazione dei dati personali - Vedi art. 17 (diritto alla cancellazione)

Condivisione di dati con terze parti - Vedi art. 7 (condizioni per il consenso), inoltre anche art. 21 (diritto di opposizione) e 22 (processi decisionali automatizzati)

Accesso illegittimo, Modifica indesiderata e Scomparsa dei dati - Vedi art. 32 (misure di sicurezza)

Vulnerabilità delle applicazioni web - Vedi art. 32 (misure di sicurezza)

Trasferimento dati non sicuro - Vedi art. 32 (misure di sicurezza)

GDPR – Processo di valutazione dei rischi

Valutazione Rischio ciclo di processo - ASL Benevento





Valutazione d'Impatto - definizione

Una **valutazione d'impatto** sulla protezione dei dati è un **processo** inteso a descrivere il trattamento,

- **valutarne la necessità e la proporzionalità**,
- a contribuire a **gestire i rischi** per i **diritti** e le **libertà** delle persone fisiche derivanti dal trattamento di dati personali,
- valutando detti rischi e determinando le misure per affrontarli**

una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità

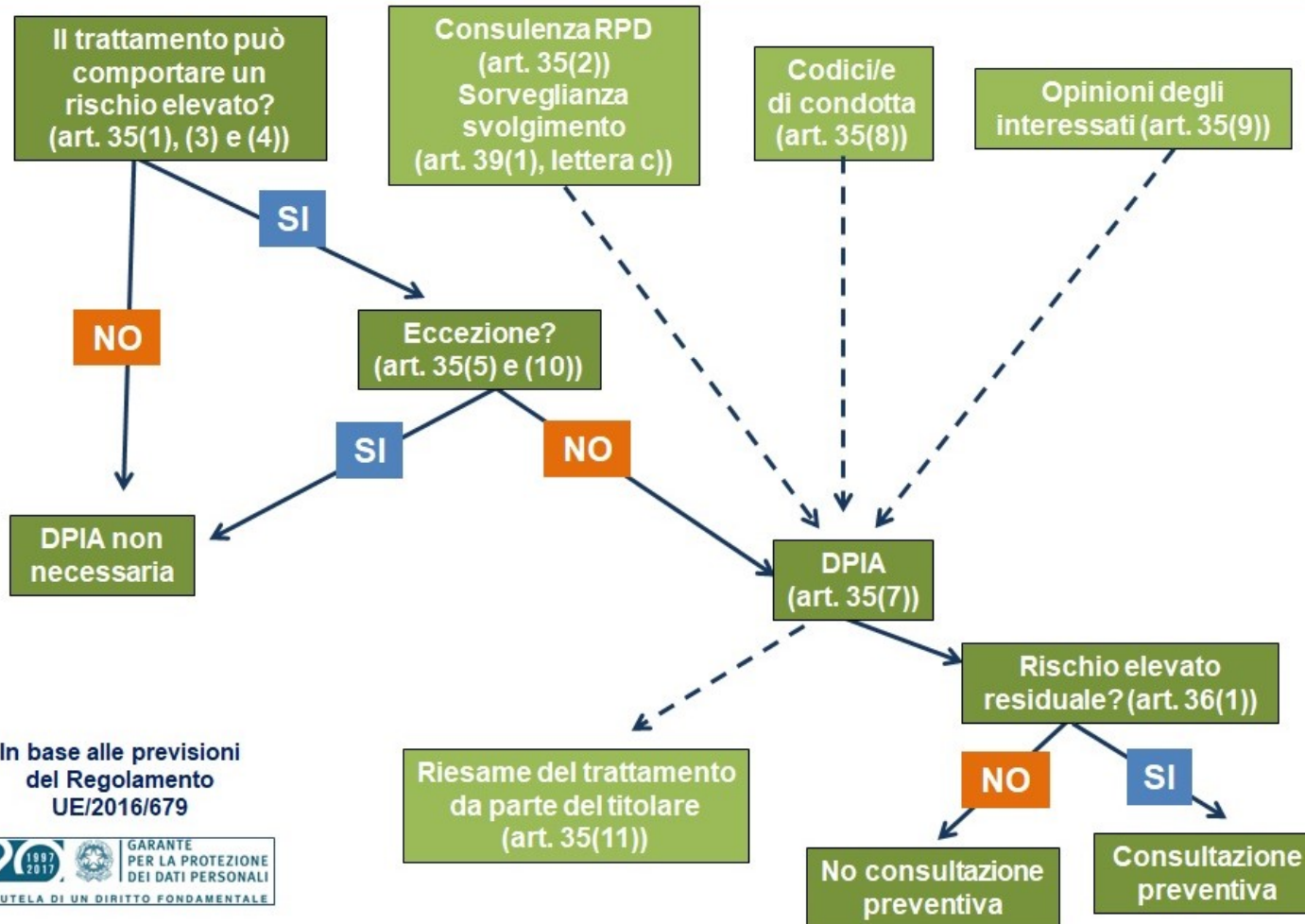


Valutazione d'Impatto - definizione

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, **non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento**. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*"

i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?





Valutazione d'Impatto – Quando ?

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento "**possa presentare rischi elevati**":

- a) una **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;
- b) il **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 1013;
- c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.



Valutazione d'Impatto – *Criteri di individuazione rischio elevato*

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione,
2. Monitoraggio sistemico
3. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente:
4. Dati sensibili o dati aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insiemi di dati
7. Dati relativi a interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
9. Quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"*

Un trattamento che **soddisfi due criteri** può formare oggetto di una valutazione d'impatto.

Maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti

Un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Valutazione d'Impatto – Quando ?

| Esempi di trattamenti | Possibili criteri applicabili | | |
|--|---|---|----|
| Un ospedale tratta i dati sanitari e genetici dei suoi pazienti | Dati sensibili ed afferenti a interessati vulnerabili | → | SI |
| Sistemi di videosorveglianza e tutor autostradali | Moderato sistematico e utilizzo di nuove tecnologie | → | SI |
| Monitoraggio delle attività svolte da un dipendente, inclusi i collegamenti ad Internet | Monitoraggio sistematico e soggetti vulnerabili coinvolti | → | SI |
| Il trattamento di profili su social media, utilizzati per sviluppare protocolli di contatto | Valutazione automatizzata di dati trattati su larga scala | → | SI |
| Una pubblicazione on-line che manda bollettini periodici ai suoi abbonati | nessuno | → | NO |
| Un sito di commercio elettronico che visualizza pubblicità afferenti a parti di ricambio per specifici apparati, analizzando gli acquisti effettuati dai clienti | Valutazione automatizzata di dati ma non sistematica o estesa | → | NO |



Valutazione d'impatto – Elementi caratterizzanti

Descrizione sistematica del trattamento (articolo 35, paragrafo 7, lettera a)):

- la natura, l'ambito di applicazione, il contesto e le finalità del trattamento
- vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
- viene fornita una descrizione funzionale del trattamento;
- sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);

Valutazione della necessità e proporzionalità (articolo 35, paragrafo 7, lettera b)):

- sono state determinate le misure previste per garantire la proporzionalità e necessità del trattamento sulla base di: **finalità determinate, esplicite e legittime**, liceità del trattamento, dati personali **adeguati e pertinenti e limitati**, **limitazione della conservazione** ;
- sono state determinate **misure che contribuiscono ai diritti degli interessati**: **informazioni** fornite all'interessato **diritto di accesso e portabilità** dei dati (articoli 15 e 20); **diritto di rettifica e alla cancellazione** (articoli 16, 17 e 19); **diritto di opposizione e di limitazione di trattamento** (articoli 18, 19 e 21);

Valutazione dei rischi per i diritti e le libertà degli interessati (articolo 35, paragrafo 7 lettera c)):

- Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi (**accesso illegittimo, modifica indesiderata e scomparsa dei dati**) : si considerano le fonti di e sono individuati gli impatti potenziali in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- sono stimate la **probabilità** e la **gravità**;
- sono determinate **le misure previste per gestire tali rischi** .



Violazione dei dati personali - Data Breach

Violazione dei dati personali (c.d. Data breach) è 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 (art. 4, punto 12 - GDPR).

Possibile cause di violazione:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Data Breach – Gli Obblighi del Titolare

Il titolare deve:

- **Notificare** la violazione all'autorità di controllo **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti** e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
- **Documenta** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue **conseguenze** e **i provvedimenti adottati per porvi rimedio**
- **Comunica la violazione all'interessato senza ingiustificato** ritardo, quando la violazione dei dati personali **è suscettibile di presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento (non obbligatoria se **intraprese misure** - pre o post violazione- adeguate a **contenere il rischio non elevato** oppure **sforzi spropositati**)



Data Breach – Gli Obblighi del Titolare

NOTIFICA al Garante

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





Data Breach – Fasi del processo di gestione

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso nelle seguenti quattro fasi:

1 - Identificazione e indagine preliminare: A seguito di ricezione della segnalazione da parte di uno degli attori, il Titolare del trattamento, per il tramite del Responsabile Ufficio Privacy effettua la registrazione e l'identificazione univoca della segnalazione, quindi, con il supporto del Responsabile della Protezione Dati, effettua una valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach (violazione)*

2 - Risk assessment e individuazione misure: nel caso si stabilisca che una possibile violazione è effettivamente avvenuta, il Responsabile Protezione Dati e, in caso di *violazioni informatiche*, l'Amministratore di sistema, devono stabilire congiuntamente le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare, se la violazione ricade nei casi in cui è necessario notificare all'Autorità Garante per la Protezione dei dati personali se l'entità della violazione necessita di comunicare l'accadimento agli interessati.

3 - Notifica all'Autorità Garante: se è stata verificata la necessità di effettuare la notifica della *violazione dei dati*, il Titolare del trattamento della ASL Benevento provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

4 - Comunicazione agli interessati: se è stata valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, in quanto è stato riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, provvederà alla comunicazione all'Interessato senza ingiustificato ritardo

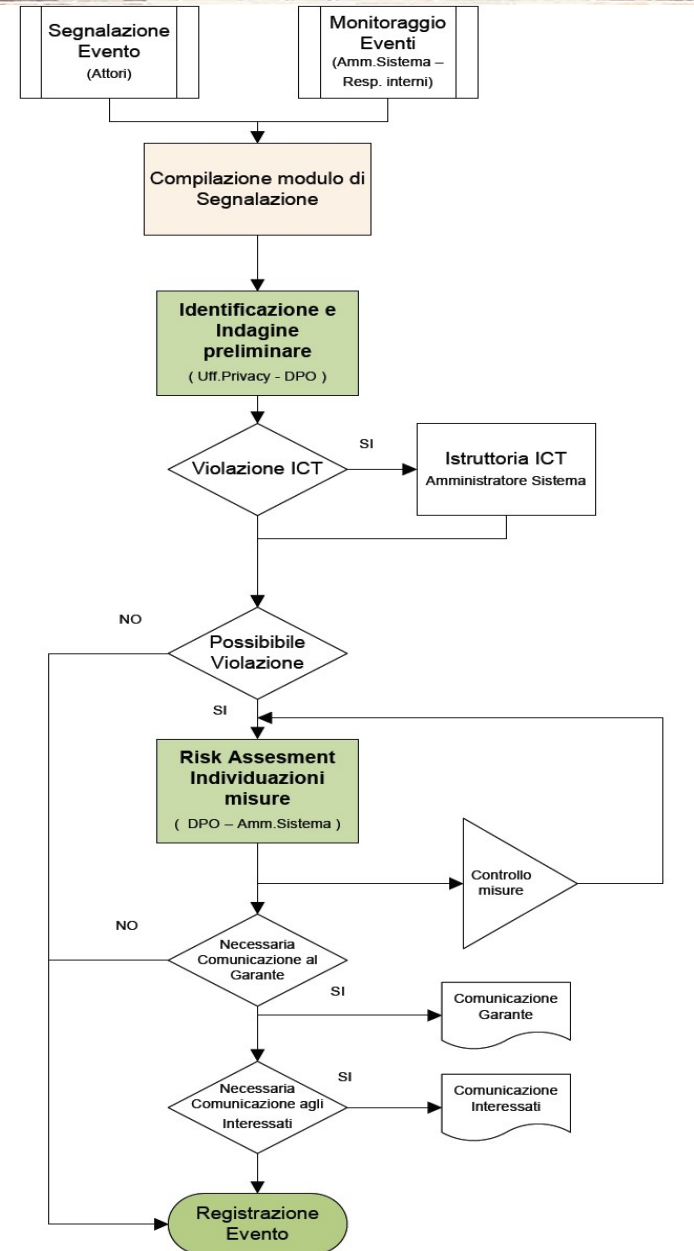


PRO.M.I.S.

Programma Mattone Internazionale Salute

Gestione del Data Breach

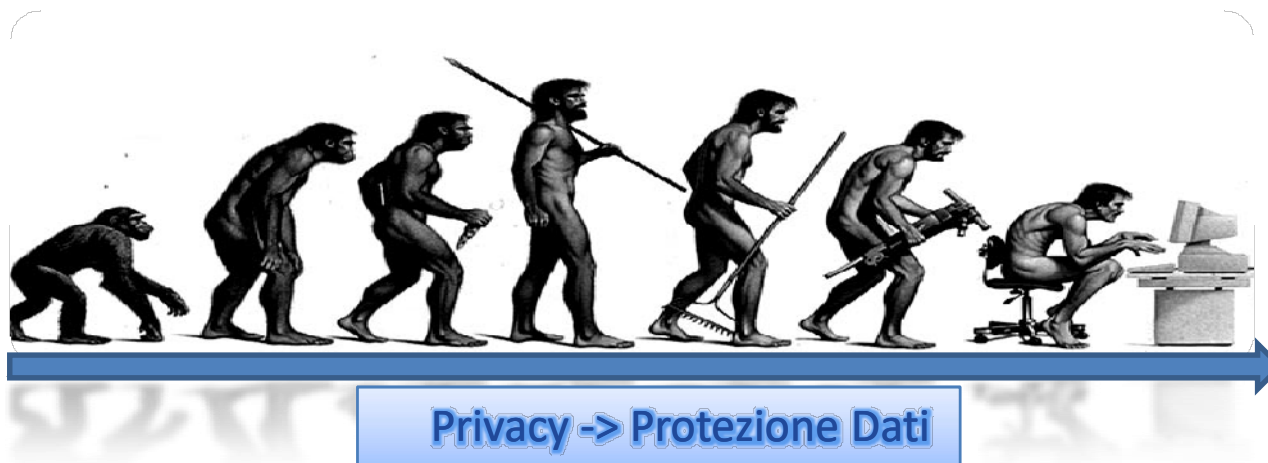
Diagramma di flusso



Conclusioni



l'oggetto del desiderio: una originale caffettiera del masochista. Design: Jacques Carlmann





PRO.M.I.S.
Programma Mattone Internazionale Salute

GRAZIE PER L'ATTENZIONE

Alberto Lombardi