STUDIO LEGALE
Villa Isoldi
& ASSOCIATI

ROMA Via Cassiodoro 1A - 00193
MILANO C.so C. Colombo 10 - 20144
+39 06.68136714 - +39 06.45666430
w.dicicco@studiolegalevillaisoldi.it
www.studiolegalevillaisoldi.it

Ordine degli avvocati di Roma – 13 gen. 2021

"Le attività richieste per la Data Protection Impact Assessment"

Avv. William Di Cicco

Definizione

Una valutazione d'impatto sulla protezione dei dati è un ***processo*** *inteso a* ***descrivere il trattamento, valutarne la necessità e la proporzionalità****, nonché 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****.*

(tratto da: "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati*" adottate dal Gruppo di Lavoro Articolo 29 il 4 aprile 2017 e modificate il 4 ottobre 2017

Contenuti minimi (artt. 35 e 36 GDPR)

a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Descrizione del contesto

Descrizione dei trattamenti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento:

Qual è il trattamento in considerazione?
Quali sono le tipologie di dati personali trattati?
Quali sono le finalità e le basi giuridiche del trattamento?
Quali sono gli strumenti e le risorse a supporto del trattamento?
Dove avviene il trattamento?
Quali sono le categorie di soggetti interessate?
Chi sono i destinatari dei dati?

A che punto siamo...

a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Valutazione della necessità e proporzionalità

Fornire una valutazione della necessità e della proporzionalità del trattamento:

Quali sono le finalità e la base giuridica del trattamento?
I dati personali raccolti e le operazioni di trattamento svolte sono necessarie per raggiungere le finalità e gli scopi della base giuridica?
Il trattamento risponde efficacemente a questa esigenza?
Il trattamento è l'alternativa meno intrusiva dal punto di vista dei diritti fondamentali per raggiungere questo scopo (necessità)?
C’è un bilanciamento fra i vantaggi del trattamento e i rischi posti dal trattamento stesso per i diritti fondamentali degli interessati (proporzionalità)?

A che punto siamo...

Fatto!

Fatto!

a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Valutazione dei rischi

Valutazione dei rischi per i diritti e le libertà degli interessati

Livello impatto

Identificazione minacce

Valutazione probabilità di accadimento

Valutazione dei rischi

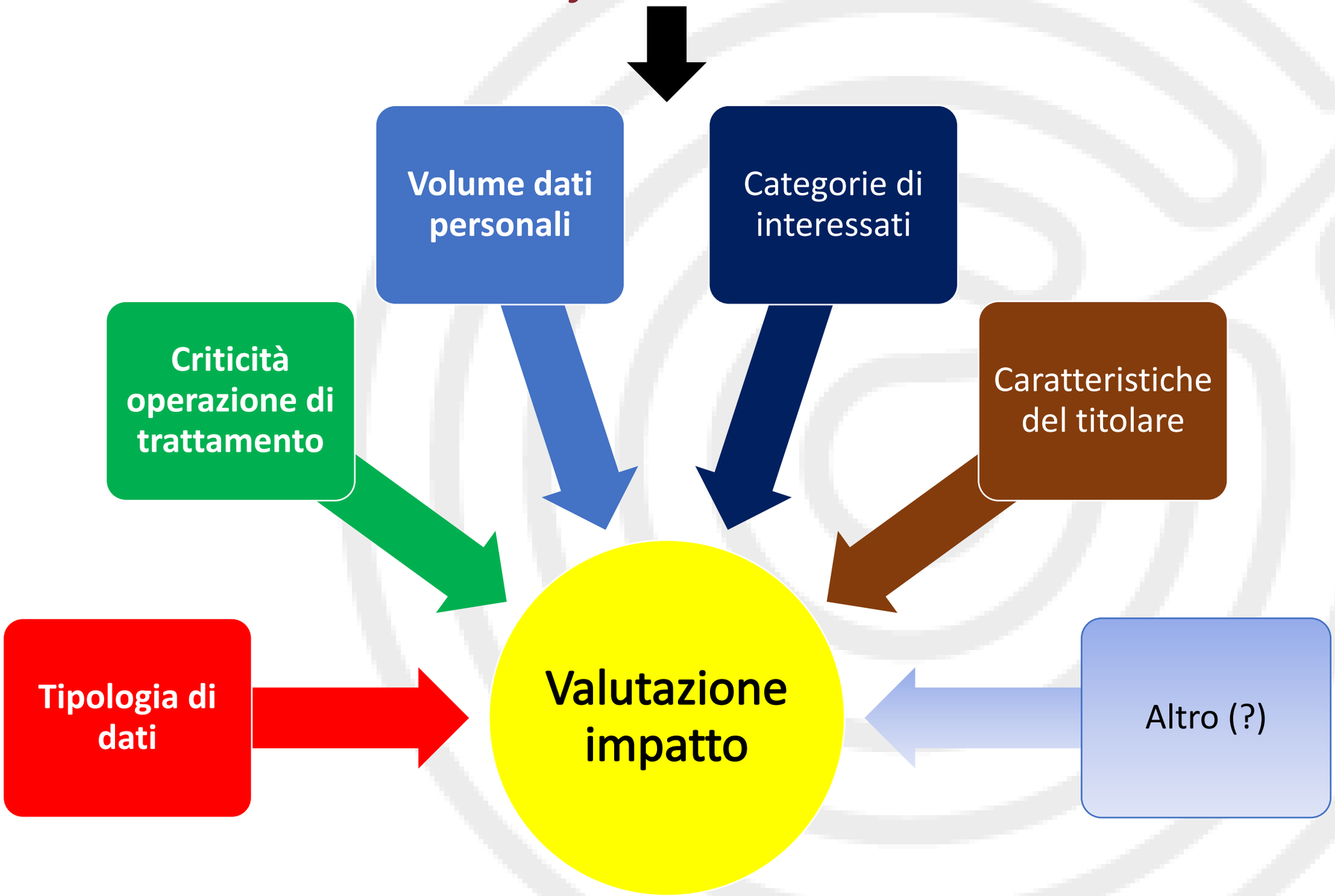
Livello impatto 1/3

Determinare il livello di impatto per i diritti e le libertà degli interessati

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono andare incontro a **disagi minori**, che supereranno senza alcun problema (tempo trascorso per rinviare informazioni e documenti, fastidi, irritazioni, ecc.).
MEDIO	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, impossibilità temporanea ad accedere a servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdita o appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	Gli individui possono subire **conseguenze significative, o addirittura irreversibili**, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Livello impatto 2/3

Considerare i fattori determinanti:



Livello impatto 3/3

Determinare il grado di impatto per i diritti e le libertà degli interessati in caso di:

EVENTO	GRADO IMPATTO
divulgazione non autorizzata dei dati personali **(perdita di RISERVATEZZA)**	❑ Basso ❑ Medio ❑ Alto ❑ Molto alto
alterazione non autorizzata dei dati personali **(Perdita di INTEGRITÀ)**	❑ Basso ❑ Medio ❑ Alto ❑ Molto alto
distruzione o perdita non autorizzata di dati personali **(Perdita di DISPONIBILITÀ)**	❑ Basso ❑ Medio ❑ Alto ❑ Molto alto

Definizione delle minacce

Identificare possibili minacce correlate al contesto complessivo del trattamento dei dati personali:

Minacce INTERNE all'organizzazione

Minacce ESTERNE all'organizzazione

Umane
(Volontarie e non volontarie)

Non umane

Probabilità accadimento minacce

Valutare la probabilità che le minacce identificate si verifichino nelle varie aree di svolgimento del trattamento dei dati personali:

Risorse di rete e tecniche
(hardware e software)

Procedure di trattamento dei dati

Risorse coinvolte nel trattamento

Settore di operatività e scala del trattamento

(Altro) …

Risorse di rete e tecniche (hardware e software)

Valutare la probabilità che le minacce identificate si verifichino in tale area:

RISORSE DI RETE E TECNICHE	
Parte del trattamento è eseguito tramite Internet o il sistema è interconnesso con un altro sistema o servizio IT esterno?	SI medio/alto
È previsto l'accesso al sistema interno tramite Internet a determinati utenti o gruppi di utenti (p. es. aree riservate)?	
Non è prevista una programmazione degli interventi di manutenzione, aggiornamento e implementazione degli strumenti hardware e software?	NO basso
Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	

Procedure di trattamento dei dati

Valutare la probabilità che le minacce identificate si verifichino in tale area:

PROCEDURE DI TRATTAMENTO DEI DATI	
I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti?	SI medio/alto
Le modalità di utilizzo della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è chiaramente definito?	
Dipendenti e collaboratori sono autorizzati a portare e utilizzare i propri dispositivi personali per connettersi al sistema di trattamento dei dati personali?	
Dipendenti e collaboratori sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO basso
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	

Risorse coinvolte nel trattamento dei dati

Valutare la probabilità che le minacce identificate si verifichino in tale area:

RISORSE COINVOLTE NEL TRATTAMENTO DEI DATI	
Il trattamento dei dati personali è eseguito da un numero non definito di persone (dipendenti, collaboratori, clienti, tecnici, ecc.)?	SI ↑ medio/alto
Parte delle operazioni di trattamento dei dati è eseguita da soggetti esterni (società di servizio, responsabile del trattamento, ecc.)?	
Gli obblighi e i compiti delle persone coinvolte nel trattamento dei dati personali sono chiaramente definiti?	
Le risorse coinvolto nel trattamento di dati personali è adeguatamente formato e informato sui compiti da svolgere e sulla potezione dei dati?	NO ↓ basso
Le risorse coinvolto nel trattamento di dati personali possono accedere solo ai dati e alle operazioni di trattamento di loro competenza (p.es. profilazione degli accessi, aggiornamento delle utenze, ecc.)?	

Settore di operatività e scala di trattamento

Valutare la probabilità che le minacce identificate si verifichino in tale area:

SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
Il proprio settore di operatività è esposto agli attacchi informatici?	SI ↑ medio/alto
L'organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi anni?	
L'organizzazione ha ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico utilizzato per il trattamento di dati personali negli ultimi anni?	
Le operazioni di trattamento riguardano un grande volume di individui e/o dati personali?	NO ↓ basso
Esistono best practice o standard di sicurezza specifiche per il proprio settore di operatività che non sono state adeguatamente seguite?	

Grado di probabilità complessiva

AREA DI VALUTAZIONE	PROBABILITÀ
RISORSE DI RETE E TECNICHE	1. Basso 2. Medio 3. Alto
PROCEDURE DI TRATTAMENTO DEI DATI	1. Basso 2. Medio 3. Alto
RISORSE COINVOLTE NEL TRATTAMENTO DEI DATI	1. Basso 2. Medio 3. Alto
SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	1. Basso 2. Medio 3. Alto

SOMMA PUNTEGGIO PROBABILITÀ	LIVELLO
da 4 a 5	Basso
da 6 a 8	Medio
da 9 a 12	Alto

Valutazione del rischio

IMPATTO

PROBABILITÀ

	Basso	Medio	Alto/Molto alto
Basso			
Medio			P
Alto			

Basso

Medio

Alto

A che punto siamo...

Fatto!

a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

Fatto!

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

Fatto!

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

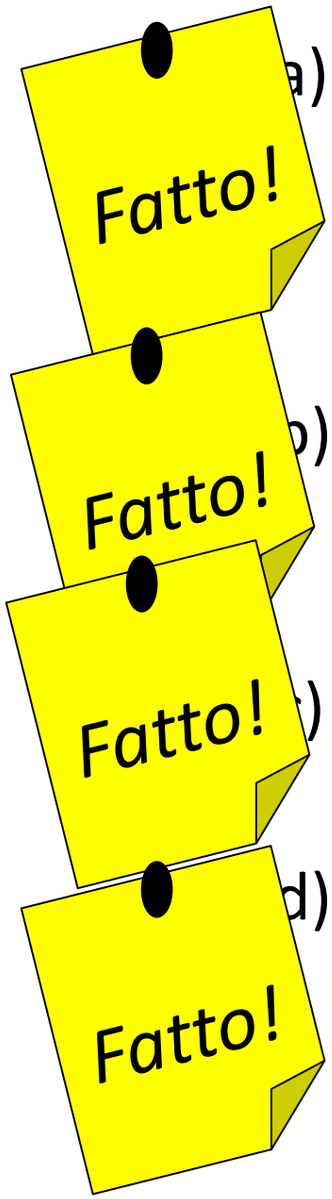
e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Misure di sicurezza

Identificare le misure tecniche e organizzative previste o pianificate:

- **Controllo degli accessi (fisici e logici)**
- **Crittografia**
- **Backup**
- **Formazione e informazione**
- **Definizione organigramma e profili utenti**
- **Minimizzazione dei dati**
- **Misure contro intrusioni esterne**
- **Manutenzione strumenti**
- **Misure contro eventi naturali**
- **... (Altro)**

A che punto siamo...



a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Applicando le misure previste...

IMPATTO

PROBABILITÀ

	Basso	Medio	Alto/Molto alto
Basso	A		
Medio		B	P
Alto			

A che punto siamo...

Fatto!

a) una **descrizione sistematica** dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

Fatto!

b) una **valutazione della necessità** e **proporzionalità** dei trattamenti in relazione alle finalità;

Fatto!

c) una **valutazione dei rischi** per i diritti e le libertà degli interessati;

Fatto!

d) le **misure tecniche e organizzative** previste o pianificate per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali;

Fatto!

e) Valutare il **livello di rischio residuo** dopo l'applicazione delle misure previste o pianificate.

Consultazione preventiva (Art. 36 GDPR)

Il titolare del trattamento, prima di procedere al trattamento, **consulta l'autorità di controllo** qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un **rischio elevato** in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Documentazione e Riesame

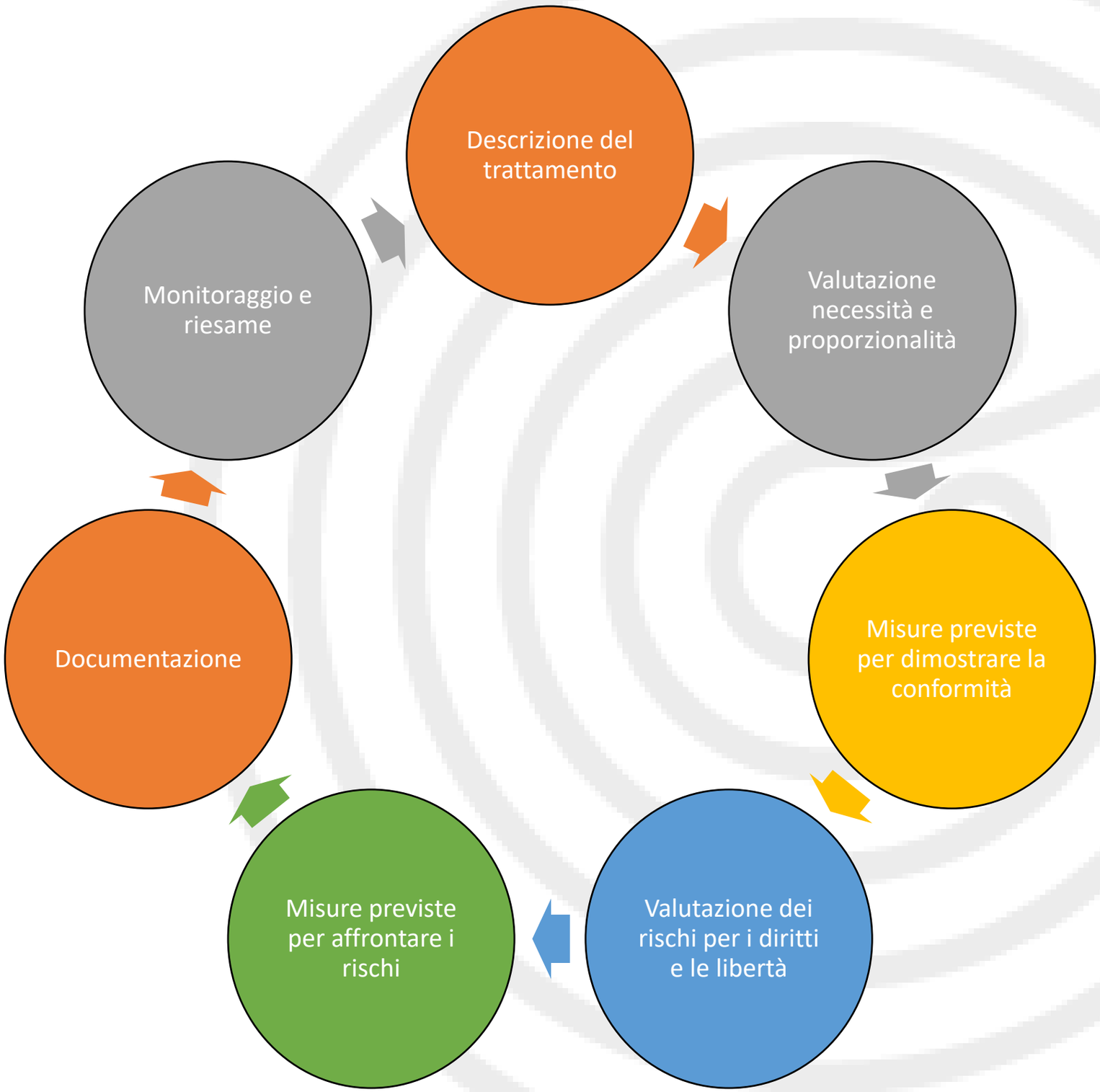
Documentare la valutazione di impatto

Non vi è l'obbligo di pubblicare la valutazione d'impatto, ma deve essere comunicata all'autorità di controllo in caso di consultazione preventiva o su richiesta da parte delle autorità competenti per la protezione dei dati personali.

Riesame

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento (articolo 35, comma 11).

Processo continuo



Quando è obbligatoria 1/2

Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto
Trattamenti valutativi, di scoring su larga scala, o trattamenti che comportano la profilazione degli interessati su aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
Trattamenti automatizzati per assumere decisioni che producono "effetti giuridici" oppure che incidono significativamente sull'interessato
Trattamenti che prevedono un utilizzo sistematico di dati per **l'osservazione, il monitoraggio o il controllo** degli interessati
Trattamenti su **larga scala di dati aventi carattere estremamente personale** (vita familiare o privata, comunicazioni riservate, dati che incidono sull'esercizio di un diritto fondamentale, dati finanziari, ecc.)
Trattamenti effettuati nell'ambito del **rapporto di lavoro** mediante sistemi tecnologici (sistemi di videosorveglianza e di geolocalizzazione) 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)

Quando è obbligatoria 2/2

Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto
Trattamenti effettuati attraverso l'uso di **tecnologie innovative**, anche con particolari misure di carattere organizzativo (es. IoT, sistemi di intelligenza artificiale, assistenti vocali on-line, dispositivi wearable, wi-fi tracking)
Trattamenti che comportano lo **scambio tra diversi titolari di dati su larga scala con modalità telematiche**
Trattamenti di dati personali effettuati mediante **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 categorie **particolari di dati** oppure di dati relativi a **condanne penali e a reati** interconnessi con altri dati personali raccolti per finalità diverse
Trattamenti sistematici di **dati biometrici**
Trattamenti sistematici di **dati genetici**

STUDIO LEGALE
Villa Isoldi
& ASSOCIATI

Avv. William Di Cicco

w.dicicco@studiolegalevillaisoldi.it

ROMA Via Cassiodoro 1A - 00193

MILANO C.so Cristoforo Colombo 10- 20144

+39 06.68136714 +39 06.45666430

www.studiolegalevillaisoldi.it

Grazie
per
l'attenzione !