VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI
TRATTAMENTO "GESTIONE SEGNALAZIONI E RECLAMI *WHISTLEBLOWING*"
(art. 35 Regolamento europeo 679/2016)

Che cos'è la valutazione di impatto?
La valutazione di impatto sulla protezione dei dati, di seguito in sigla DPIA, è una procedura intesa a descrivere un trattamento, a valutarne la necessità e la proporzionalità nonché a valutarne i rischi per i diritti e libertà delle persone fisiche, allo scopo di determinare le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo.

A cosa serve condurre la valutazione di impatto?
La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del Regolamento Europeo 679/2016 ma anche ad attestare di aver adottato misure idonee a garantire tali prescrizioni.

Chi deve condurre la DPIA?
La conduzione della DPIA spetta al titolare del trattamento, consultandosi con il responsabile della protezione dei dati e acquisendo, se necessario, le informazioni di settore presso l'amministratore di sistema, il fornitore del software/servizio e del responsabile del servizio che si occupa dell'attività di trattamento.

Quando va condotta la DPIA?
Laddove possibile, la DPIA dev'essere condotta prima di procedere al trattamento. Dovrebbe comunque essere previsto un riesame continuo della DPIA, in quanto i trattamenti tendono a evolvere rapidamente e possono facilmente presentarsi nuove vulnerabilità; pertanto, occorre osservare che la revisione di una DPIA non è soltanto utile ai fini del miglioramento continuo, ma è anche indispensabile per mantenere inalterato il livello di protezione dei dati al mutare delle condizioni nel tempo.

In quali casi la DPIA è obbligatoria?
La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".
L'articolo 35 del GDPR indica i criteri in base ai quali si individuano i casi nei quali la DPIA è necessaria:

1. il trattamento determina 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;
2. il trattamento riguarda dati particolari su larga scala;
3. il trattamento riguarda la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Inoltre, il Garante italiano, insieme alle altre autorità europee ha predisposto, con provvedimento n. 467 dell'11 ottobre 2018, un *Elenco delle tipologie di trattamenti, […] da sottoporre a valutazione d'impatto*. Sinteticamente l'elenco prevede tali ipotesi:

4. Trattamenti valutativi o di scoring effettuati su larga scala, profilazione, attività predittive;
5. Trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure tali da incidere in modo significativo sull'interessato, come impedire l'esercizio corretto di un diritto o di avvalersi di un bene o di un servizio o di poter continuare ad essere parte di un contratto in essere (ad es. lo screening effettuato sui clienti di una banca attraverso l'utilizzo dei dati registrati in una centrale rischi);
6. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati online o con App, il trattamento di dati identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione, e i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati anche per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc;
7. Trattamenti su larga scala di dati aventi carattere estremamente personale (come definiti nelle Linee Guida), compreso dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
8. 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;
9. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
10. Trattamenti effettuati attraverso l'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 testuale; monitoraggi effettuati da dispositivi wearable, cioè indossabili quali, ad esempio,

gli smartwatch o gli stessi smartphone attraverso i software di assistenza e comando vocale, ndr.); tracciamenti di prossimità come ad es. il wi-fi tracking;

11. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
12. 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. pagamenti effettuati tramite tecnologia mobile);
13. Trattamenti di categorie particolari di dati oppure di dati relativi a condanne penali e a reati di cui all'art. 12 interconnessi con altri dati personali raccolti per finalità diverse;
14. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento
15. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Infine, in caso di dubbi il titolare potrà sempre rivolgersi alle Autorità di controllo per una consultazione preventiva sulla necessità o meno di effettuare la valutazione di impatto (art. 36).

PREMESSE METODOLOGICHE

Con il Regolamento europeo 679/2016 il legislatore ha posto tra i principi cardini dell'ordinamento in materia di trattamento dei dati personali un approccio basato sulla responsabilizzazione del titolare. Si affida al Titolare il compito e la responsabilità, di valutare il rischio relativo al trattamento dei dati personali per i diritti e le libertà delle persone fisiche e l'adozione delle misure adeguate a rendere il trattamento conforme ai principi in materia. Il Regolamento prevede che i titolari del trattamento attuino misure adeguate a garantire ed essere in grado di comprovare il rispetto dello stesso, tenendo conto, tra l'altro, dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1).

La valutazione di impatto sulla protezione dei dati, di seguito in sigla DPIA è un processo inteso a descrivere il trattamento, a valutarne la necessità e la proporzionalità, a contribuire a gestire i rischi per i diritti e libertà delle persone fisiche, valutando tali rischi e determinando le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo.

La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Quindi, perché la DPIA è obbligatoria per questa attività di trattamento?

Come chiarito di recente dal Garante proprio con riferimento ai trattamenti effettuati mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite (v. provv. 10 giugno 2021, n. 235, doc. web n. 9685922, spec. par. 3.3), il trattamento dei dati personali effettuati in tale ambito – in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore (tanto a livello nazionale quanto a livello europeo, cfr., da ultimo, la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione) – presenta rischi specifici per i diritti e le libertà degli interessati.

Il 9 marzo 2023 il Consiglio dei Ministri ha approvato in via definitiva il decreto legislativo che recepisce la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, la cd. direttiva whistleblowing.

L'art. 13 del predetto decreto legislativo sancisce che: "*1. Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE) 2018/1725.*

2. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

3. I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

4. I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4, in qualità di titolari del trattamento, nel rispetto dei princìpi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

5. I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.

6. I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi

*derivanti dai trattamenti effettuati, **sulla base di una valutazione d'impatto sulla protezione dei dati**, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018"*.
Ciò, anche considerata, la "vulnerabilità" degli interessati (soggetti segnalanti e segnalati) nel contesto lavorativo alla luce degli artt. 35 e 88, par. 2, del Regolamento UE 2016/679 e delle "*Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del Regolamento 2016/679*", WP 248 del 4 aprile 2017 e, da ultimo, del provvedimento 4 dicembre 2019, doc. web n. 9215763, con il quale il Garante ha reso il parere ad ANAC sullo schema di "*Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001 (c.d. whistleblowing)*", ove espressamente si fa rinvio "*ai principali adempimenti previsti dalla normativa in materia di protezione dei dati personali (artt. 13, 14, 30, 35 e 36 del Regolamento), anche tenuto conto degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo*".

1. Descrizione sistematica del trattamento

L'Ente si è adeguato a quanto disposto dalle Linee guida ANAC numero 469 del 9 giugno 2021, *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)*.
A partire dal 2021 infatti, l'invio della segnalazione può essere effettuato solo in modalità informatica, avvalendosi di un'applicazione web dedicata, in quanto sono stati considerati non capaci di garantire la riservatezza necessaria questi altri metodi;

Nel registro delle attività di trattamento dei dati dell'Ente, l'attività di trattamento viene censita in tale maniera:

- *attività di trattamento:* gestione delle segnalazioni di presunti illeciti effettuate tramite piattaforma informatica);
- *finalità:* garantire un canale di comunicazione riservato per la denuncia di fatti di natura corruttiva e comunque irregolari;
- *base giuridica:* d.lgs. 24/2023;
- *tipologia di dati trattati*: dati personali anagrafici e di recapito del segnalante e dati personali dei soggetti oggetto della segnalazione e dati giudiziari;
- *categorie di interessati*: dipendenti, collaboratori, consulenti, fornitori, tirocinanti, persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, soggetti oggetto della segnalazione e RPCT;
- *categorie di destinatari*: RPCT, Autorità giudiziaria, ANAC, soggetto che esercita il potere disciplinare;
- *strumenti utilizzati*: https://comunecavedine.cctwhistleblowing.it/#/
- *responsabili esterni*: Servizio Whistleblowing - Consorzio dei Comuni Trentini;
- *luogo di conservazione dei dati*: Trento (server di Trentino Digitale S.p.A.), all'interno dello Spazio Economico Europeo;
- *tempi di conservazione*: I dati saranno trattati per tutta la durata della gestione della segnalazione e, in seguito, saranno conservati per il tempo necessario all'accertamento della fondatezza della segnalazione e, se del caso, all'adozione di provvedimenti disciplinari conseguenti e/o all'esaurirsi di eventuali contenziosi, avviati a seguito della segnalazione o allo spirare dei termini per proporre impugnazione. Ai sensi dell'art. 14 del D. lgs. 24/2023, le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
- *misure di sicurezza*: il titolare ha definito il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018.
- *modalità di informazione dell'interessato*: l'Ente ha predisposto un'informativa specifica disponibile alla voce *Privacy* del sito istituzionale e disponibile all'interessato che accede all'applicativo ma prima di aver inserito la segnalazione (quindi prima di aver inserito i propri dati personali). Inoltre, l'Ente rende disponibile il link alla piattaforma whistleblowing nei contratti dei nuovi dipendenti, dei lavoratori somministrati e di tutti coloro che prestano la propria attività lavorativa a favore dell'Ente.

2. Elenco della documentazione adottata e posta alla base della DPIA:

- ✓ Procedura indicante le modalità di segnalazione, prot. 8281 dd. 04.09.2023
- ✓ Nomina a responsabile del trattamento a Consorzio dei Comuni Trentini soc. coop. prot. 8966 dd. 20.09.2023
- ✓ Misure di sicurezza relative alla piattaforma informatica, prot. 8061 dd. 28.08.2023
- ✓ Nomina all'amministratore di sistema, prot. 5049 dd. 24.05.2023
- ✓ Misure di sicurezza ICT adottate dall'Ente adottate con delibera G.C. n. 144 dd. 19.09.2023

- ✓ Nomina RPCT prot. 3383 dd. 08.04.2013
- ✓ Codice di comportamento, adottato con deliberazione di Giunta Comunale n. 167 del 19.12.2022

3. Valutazione della necessità e proporzionalità del trattamento

*Descrizione degli elementi che comprovano la finalità di **garantire un canale di comunicazione riservato per la denuncia di fatti di natura corruttiva e comunque irregolari**, con la specifica degli indicatori di necessità e di proporzionalità del trattamento.*

VALUTAZIONE	DESCRIZIONE	Sì	NO	DA FARE
della necessità del trattamento	Le finalità sono:			
	- Specifiche e determinate	X		
	- Legittime (cioè fondate su base giuridica o compiti istituzionali)	X		
della proporzionalità del trattamento	I dati risultano pertinenti e adeguati alle finalità e limitati a quanto necessario	X		
	I dati sono esatti e aggiornati	X		
	Il periodo di conservazione dei dati è limitato (sulla base di norme di legge)	X		
	I rapporti con i responsabili esterni del trattamento sono disciplinati da atto giuridico	X		
in merito al trasferimento dati	I dati personali sono comunicati in ambito europeo	X		
	I dati personali sono comunicati in ambito extraeuropeo (con le dovute garanzie)		X	
	I dati personali sono diffusi/pubblicati		X	
del rispetto dei diritti degli interessati	L'interessato è informato circa il trattamento dei dati effettuato mediante un'informativa adeguata, resa nei modi stabiliti	X		
in merito alla gestione dei trattamenti	Il personale, in merito al trattamento dati, è istruito?	X		
	Il personale, in merito al trattamento dati, è autorizzato?	X		

4. Valutazione dei rischi per i diritti e le libertà degli interessati[1]

Il titolare, compilando il file Excel allegato, descrive e valuta i rischi connessi al trattamento per i diritti e le libertà degli interessati, adottando questo metodo:

[1] Quali sono le informazioni da considerare nella valutazione del rischio? Le informazioni necessarie per valutare il rischio derivano da diverse fonti come l'esperienza, la documentazione di incidenti già avvenuti, consulenze e pareri, documentati alla voce "note" del file Excel "analisi dei rischi". A tal fine viene indicata nel campo "note", la documentazione e le procedure considerate/contemplate nell'assegnazione dei valori di impatto e probabilità.
Come viene calcolato il rischio? Il rischio viene calcolato come il prodotto della probabilità di una vulnerabilità (ovvero di una violazione di una delle proprietà della sicurezza: riservatezza – integrità – disponibilità) moltiplicato per l'impatto determinato dallo sfruttamento della stessa vulnerabilità (rispetto al diritto alla protezione dei dati personali). Esprimendo il concetto in formula il rischio viene così espresso

Rischio = ProbViolazione * ImpViolazione

Secondo un approccio standard in letteratura, il processo di valutazione richiede una quantificazione secondo scale con intervalli discreti con associato un significato intuitivo per la valutazione della probabilità e dell'impatto. Le scale adottate sono le seguenti:

Probabilità che si verifichi una violazione di riservatezza, integrità, disponibilità
1 evento raro (probabilità bassa)
2 evento improbabile (probabilità moderata)
3 evento possibile (probabilità elevata)
4 evento probabile (probabilità più che elevata)
5 evento quasi certo (probabilità elevatissima)

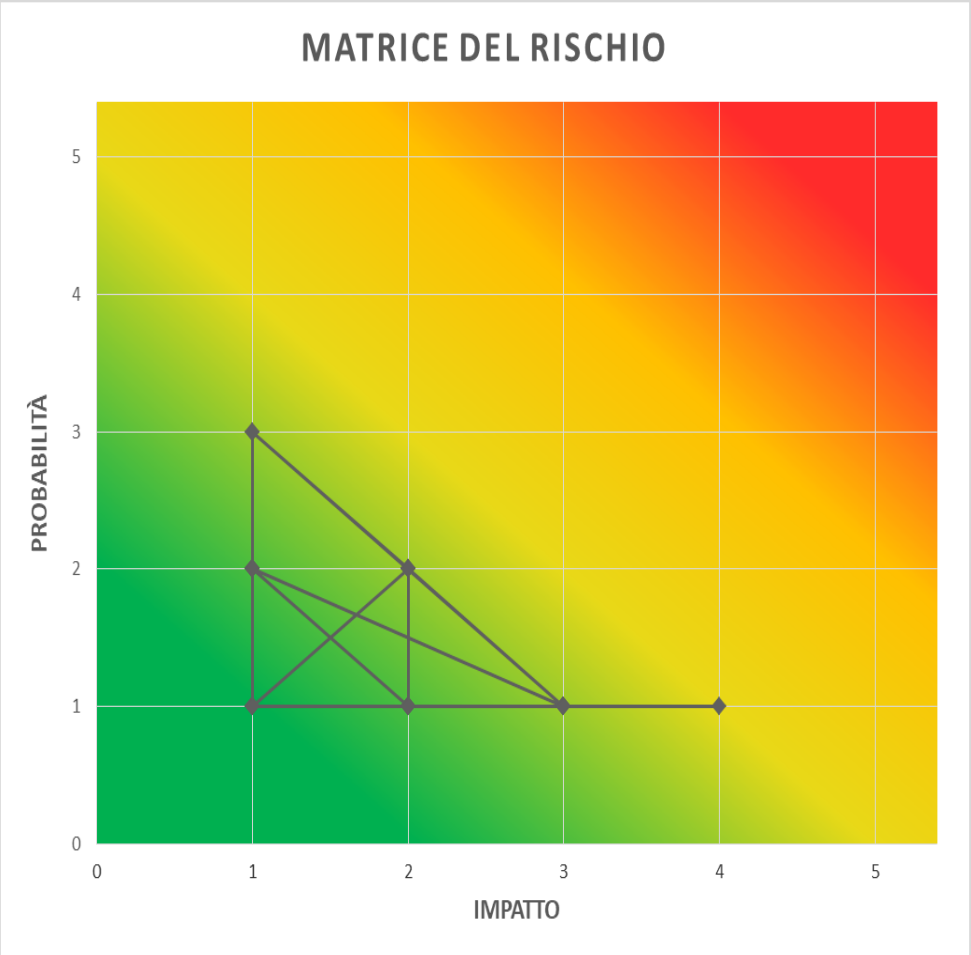
Impatto della violazione di riservatezza, integrità, disponibilità
1 impatto insignificante
2 impatto modesto
3 impatto moderato
4 impatto importante
5 impatto elevato

L'utilizzo delle scale descritte consente di costruire una matrice del rischio che permette di suddividere il rischio stesso in quattro classi: basso = verde (valori da 1 a 3), giallo=medio-basso (valori da 4 a 6), arancione=medio-elevato (valori da 8 a 12) ed alto=rosso (da 15 a 25) come mostrato nella Matrice del rischio.

- Ipotizza degli eventi/violazioni di dati, individuando quale possa essere la minaccia specifica;
- Ipotizza quale può essere l'impatto dell'evento sui diritti dell'interessato, utilizzando una scala da 1 a 5, dove 1 equivale a "impatto insignificante" e 5 equivale a "impatto elevato";
- Ipotizza quale può essere la probabilità che un evento/violazione di dati si verifichi, su una scala da 1 a 5, dove 1 equivale a "evento raro (probabilità bassa)" e 5 equivale a "evento quasi certo (probabilità elevatissima)".
- Nell'assegnazione dei valori l'Ente ha tenuto conto delle misure di sicurezza già adottate e poste in essere, che ha elencato alla voce "Note".

Compilando il file Excel Valutazione del rischio (Allegato 1 primo foglio), cioè la tabella degli eventi e delle relative violazioni, viene calcolato automaticamente il grado di rischio su una scala da 1 a 25, dove 1 equivale a un rischio minimo e 25 equivale al rischio più elevato, ed avere immediata evidenza delle minacce maggiormente rischiose.

Gli esiti della compilazione vengono riportati automaticamente nella seguente tabella "matrice del rischio" e nella tabella che riporta il numero totale delle minacce per ciascun livello di rischio.



Entità del rischio	Valori di riferimento	Numero minacce
Basso/accettabile	Da 1 a 3	32
Medio-basso	Da 4 a 6	5
Medio-alto/rilevante	Da 8 a 12	0
Alto/elevato	Da 15 a 25	**0**

5. Esito della compilazione del foglio Excel denominato "Analisi dei rischi"

Il risultato finale e complessivo della valutazione dei rischi connessi al trattamento si colloca nelle celle arancioni o gialle o verdi significa che il trattamento non presenta un livello elevato di rischio generale per i diritti e le libertà degli interessati.
Il titolare, quindi, non è obbligato a introdurre o adottare nuove misure di sicurezza ma può farlo al fine di mitigare e abbassare ulteriormente il rischio.

6. Consultazione del Responsabile della Protezione dei Dati

Il titolare si consulta con il Responsabile Protezione Dati che, in data 6 ottobre 2023 prot. n. 9499 ha fornito parere

positivo con prescrizioni

7. Risultato della Valutazione d'impatto sulla protezione dei dati

A. Il titolare del trattamento, effettuata la Valutazione di impatto sulla protezione dei dati del trattamento valuta di aver adottato le misure tecniche e organizzative adeguate a garantire il livello di sicurezza adeguato ai rischi connessi al trattamento e ritiene quindi che il trattamento sia conforme alla normativa vigente in materia di trattamento dei dati personali.

Cavedine, 11 ottobre 2023

IL SINDACO

ANGELI
DAVID
11.10.2023
13:05:04
GMT+00:00