Comune di Portobuffolé

Provincia di Treviso

Protocollo e Data come da segnatura

Documento di valutazione di impatto sui diritti e le libertà degli interessati oggetto di trattamento.

Titolare del trattamento	Comune di Portobuffolè
Designato al trattamento	RPCT e Segretario comunale dott. Luca Soccorso
Trattamento sottoposto a valutazione d'impatto (D.P.I.A.)	Gestione delle segnalazioni *whistleblowing*

Introduzione

L'articolo 35 del Regolamento (UE) 2016/679, pur non fornendone una definizione puntuale, prevede l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il significato e la funzione della DPIA, tuttavia, emergono chiaramente dalle indicazioni del Gruppo di lavoro Articolo 29 (oggi EDPB – *European Data Protection Board*), che afferma:

"*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.*

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità" [1].

La DPIA si configura quindi come uno strumento essenziale per assicurare che il trattamento sia progettato e gestito in modo conforme ai principi del GDPR, consentendo al titolare di individuare tempestivamente i rischi, adottare misure adeguate e dimostrare la propria *accountability*.

Il Titolare del trattamento, considerato l'obbligo normativo di cui agli artt. 35 Regolamento (UE) 2016/679 (recante disposizioni relative alla valutazione di impatto sulla protezione del dato personale) e 13, co. 6 d.lgs. 24/2023, ha ritenuto necessario procedere ad una valutazione d'impatto sul trattamento denominato "Gestione delle segnalazioni *whistleblowing*".

[1] Cfr. "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679",* adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - WP 248 rev.01

Definizioni

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Interessato (del trattamento): soggetto al quale si riferiscono i dati personali, persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dato personale: qualsiasi informazione riguardante un interessato.

Valutazione di impatto sul dato personale: procedura prevista dall'articolo 35 del Regolamento UE/2016/679 che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. La DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Danno: effetto negativo determinato dal verificarsi di una minaccia. Il danno è causato dalla compromissione del dato personale dell'interessato nelle tre dimensioni di riservatezza, disponibilità ed integrità.

Minaccia: evento potenzialmente dannoso che, se verificato, pone in pericolo i dati personali dell'interessato, con ricadute sui suoi diritti e le sue libertà, causando un danno.

Rischio potenziale: ponderazione del danno per la probabilità statistica che l'evento avverso accada. Si tratta di un indice creato per poter confrontare eventi (in questo contesto le minacce) che hanno diverse probabilità di accadimento e diverse dimensioni del danno.

Contromisura: misura in grado di mitigare il rischio, riducendo la probabilità di accadimento della minaccia.

Vulnerabilità: rappresentano delle situazioni che innalzano la probabilità del rischio sul dato personale.

Rischio reale: è il rischio potenziale, mitigato dallo stato di protezione del dato personale, cioè, diminuito dalle contromisure già adottate e aumentato dalle vulnerabilità presenti.

Piano del trattamento del rischio: piano di progettazione operativo con il quale si individuano le contromisure da implementare, nonché il grado di maturità di quelle già attuate, necessarie per abbassare il rischio reale al di sotto della soglia "alto"

Rischio residuo: è il rischio reale, mitigato dallo stato futuro di protezione del dato personale. Esso si potrà ottenere a seguito dell'attuazione del piano del trattamento del rischio.

Figure interessate dal procedimento di valutazione d'impatto

Soggetto interessato	Funzione svolta
Soggetto designato all'analisi del trattamento sottoposto a valutazione	È il soggetto che, essendo referente del servizio il cui trattamento è sottoposto a valutazione d'impatto, viene individuato come idoneo ad effettuarla. Egli procederà a compierla rispettando tutti i criteri di cui all'art. 35, par. 7 del Regolamento (UE) 2016/679, ossia provvedendo a:

	- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; - una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; - una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e - le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Il soggetto designato allo svolgimento della presente D.P.I.A. è il RPCT del Comune di Portobuffolè.
Referente Privacy (privacy manager)	Il Titolare del trattamento, il Comune, nella persona del legale rappresentante, sindaco *pro tempore*, provvede ad individuare all'interno dell'Ente la persona che si occupa dei vari adempimenti privacy affinché il Titolare possa rispettare il principio di *accountability* (responsabilizzazione) introdotto dal Regolamento (UE) 2016/679. In ambito di D.P.I.A. egli assiste il soggetto designato all'analisi del trattamento.
Responsabile della protezione dei dati (DPO/RPD)	Art. 35, par. 2, Reg. UE 2016/679: "*Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno".* L'art. 39 Reg. UE 2016/679 prevede, tra i vari compiti affidati al DPO, par. 1, lett. c) vi sia quello di "*fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35*".

PANORAMICA DEL TRATTAMENTO (*art. 35, par. 7, lett. a) Reg. UE 2016/679*)

Il presente verbale descrive la valutazione di impatto sulla protezione del dato personale effettuata sui trattamenti come di seguito indicati.

Nella fattispecie concreta, sulla base della tipologia di trattamento eseguito, il grado di compromissione dei dati sarà considerato come la probabilità di accadimento di un una o più minacce e l'impatto derivante dal verificarsi di una minaccia in relazione ai diritti e le libertà dell'interessato. Maggiore è il grado di compromissione, maggiore sarà la probabilità di rischio per i diritti e le libertà dell'interessato.

Nella fattispecie si considerano rischi:

- Rischio che a causa del trattamento derivi un danno reputazionale all'interessato. Si pensi, in questo frangente, ad una violazione che comporti la perdita di riservatezza delle informazioni riferite alla persona fisica coinvolta.
- Rischio di discriminazione (a scuola, a lavoro, ecc.) derivante dal trattamento. Come nel precedente punto, il rischio di discriminazione può derivare dalla perdita di riservatezza del dato personale, ma anche nella menomazione della sua integrità, laddove un'informazione sia stata acquisita o registrata in modo non accurato.
- Rischio di subire un furto di identità a causa del trattamento. Tale rischio si lega specificamente alla perdita di riservatezza e di disponibilità del dato personale, ed è legato essenzialmente alla natura di bene personalissimo connessa al dato personale (che per sua natura è indisponibile).
- Rischio che il trattamento comporti delle perdite finanziarie all'interessato, valutando anche l'eventuale danno da perdita di chance laddove, ad esempio, il trattamento comporti l'esclusione dalla possibilità di gestire alcuni affari. Il rischio è sicuramente connesso alla perdita di riservatezza ed integrità dei dati personali coinvolti nel trattamento.
- Rischio di subire danni fisici o psicologici come conseguenza del trattamento; si pensi ad un ospedale che perda i dati della cartella clinica di un paziente di lì a poco soggetto ad intervento.
- Rischio di perdita del controllo dei dati, laddove l'interessato, a causa del trattamento, non possa più disporre liberamente di alcune sue informazioni personali (si pensi, ad esempio, al problema dell'acquisizione e diffusione di immagini personali da parte di un paparazzo).
- Rischio di subire svantaggi economici e sociali.
- Rischio di trovarsi nell'impossibilità di esercitare alcuni diritti. Si deve ricordare, infatti, come la tutela dei dati personali sia costituzionalmente riconosciuta come diritto prodromico al corretto esercizio di tutte le altre libertà e diritti riconosciuti dall'ordinamento (nazionale ed europeo).

Il Titolare del trattamento è chiamato ad esprimersi sulle conseguenze (impatto) che si potrebbero verificare in termini di danno (fisico, materiale, immateriale) qualora i dati personali venissero persi, distrutti e quindi non più disponibili, modificati e diffusi, ossia portati a conoscenza o comunicati a soggetti non autorizzati. In particolare, il Titolare del trattamento è chiamato ad individuare anche la probabilità che detto rischio ha di verificarsi.

Per effettuare la valutazione d'impatto con cognizione di causa, l'Ente ritiene opportuno esplicitare le minacce che potrebbero avverarsi nell'ambito dello specifico trattamento sottoposto a D.P.I.A.

Le minacce prese in considerazione sono elencate di seguito.

Elenco minacce:

- R = riservatezza; I = integrità; D = Disponibilità

MINACCIA	R	I	D
Uso non autorizzato della strumentazione	x	x	x
Alterazione volontaria e non autorizzata di dati di business	x	x	x
Virus (malware)	x	x	x

Accesso non autorizzato alla rete	x	x	x
Uso non autorizzato della rete da parte degli utenti	x	x	x
Trattamento (volontario o inconsapevole) non consentito di dati (personali)	x	x	
Importazione o esportazione illegale di software		x	x
Errori degli utenti con accesso alla piattaforma informatica	x	x	x
Uso dei servizi da parte di persone non autorizzate	x	x	x
Degrado dei media		x	x
Uso di servizi in modo non autorizzato	x	x	x
Furto identità	x	x	x
Intercettazione (inclusa analisi del traffico)	x		x
Furto di documenti o supporti di memorizzazione	x		x
Furto di apparati o componenti	x		x
Recupero di informazioni da media dismessi	x		x
Rivelazione di informazioni (da parte del personale o fornitori)	x		
Infiltrazione nelle comunicazioni		x	
Incendio		x	x
Allagamento		x	x
Polvere, corrosione, congelamento			x
Distruzione di strumentazione da parte di persone malintenzionate			x
Attacchi (bombe, terroristi)			x
Fulmini e scariche atmosferiche			x
Disturbi elettromagnetici			x
Fenomeni climatici (uragani, nevicate)			x
Terremoti, eruzioni vulcaniche			x
Perdita di energia (o sbalzi di tensione)			x
Malfunzionamento nei componenti di rete	x	x	x
Errori di trasmissione (incluso il misrouting)		x	x
Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC)			x
Interruzione di servizi erogati riconducibili ai fornitori esterni			x
Indisponibilità del personale (malattie, sciopero, ecc)			x
Perdita di fornitori, fallimento, incidenti			x
Errori dei componenti TLC	x	x	x
Danni alle linee TLC	x	x	x
Eccesso di traffico sulle linee TLC			x
Fault o malfunzionamento della strumentazione IT		x	x
Malfunzionamenti software applicativi sviluppati per i clienti		x	x
Malfunzionamenti pacchetti software usati internamente	x	x	x
Malfunzionamenti software applicativi sviluppati per uso interno	x	x	x
Errori di manutenzione hardware e software di base	x	x	x
Saturazioni dei sistemi IT	x	x	x

Elenco delle contromisure adottate dall'Ente:

- Disciplinare per la gestione del canale interno di segnalazione;
- Formazione di base del personale deputato alla gestione delle segnalazioni (sia in ambito privacy, sia in ambito anticorruzione);
- Utilizzo di credenziali sicure (lunghezza di almeno 8 caratteri) per l'accesso alla piattaforma informatica;
- Crittografia (piattaforma informatica);
- Controllo degli accessi logici (piattaforma informatica);
- Prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza (piattaforma informatica);
- I sistemi sono soggetti a backup remoto giornaliero con *policy* di *data retention* di 7 giorni necessari per finalità di *disaster recovery* (piattaforma informatica);
- Procedura per la gestione del *data breach* (Responsabile del trattamento);
- Nomina *ex* art. 28 Regolamento (UE) 2016/679 nei confronti del fornitore della piattaforma informatica deputata a ricevere le segnalazioni scritte;
- Parafulmine;

PANORAMICA DEL TRATTAMENTO

Il trattamento sottoposto a valutazione d'impatto (c.d. D.P.I.A.) riguarda la gestione delle segnalazioni in materia di *whistleblowing*; nello specifico, verrà presa in considerazione la gestione del c.d. canale di segnalazione interno, il quale consente di inoltrare le segnalazioni provenienti dal *whistleblower* (dipendenti pubblici, intesi in senso ampio e collaboratori della pubblica amministrazione), al responsabile della prevenzione e della corruzione (RPCT).

I canali di segnalazione interna messi a disposizione dall'Ente sono i seguenti:

- piattaforma informatica;

- incontro diretto con il RPCT, fissato entro un termine ragionevole (come indicato nell'atto organizzativo, la segnalazione verrà effettuata oralmente in presenza del RPCT e, successivamente, verrà redatto apposito verbale con sottoscrizione sia del segnalante sia del RPCT; una volta completata la segnalazione, il RPCT consegna copia del verbale al segnalante e provvede, con la contestuale presenza del segnalante, a riportare il contenuto del verbale all'interno della piattaforma informatica utilizzata per le segnalazioni scritte, aprendo una nuova segnalazione).

Natura dei dati

Considerato che la normativa di riferimento (d.lgs. 24/2023) stabilisce che la segnalazione consiste nella "comunicazione scritta od orale di informazioni sulle violazioni" e che per informazioni sulle violazioni si intendono tutte le "informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni", la ricezione e la gestione delle segnalazioni dà luogo al trattamento di dati personali c.d. "comuni"; può dar luogo, a seconda del contenuto delle segnalazioni e degli atti e documenti allegati, a trattamenti di dati

personali c.d. particolari (*ex* art. 9 Reg. UE 2016/679) e di dati personali relativi a condanne penali e reati (*ex* art. 10 Reg. UE 2016/679).

Ciclo di vita del trattamento

L'art. 14 del d.lgs. 24/2023, rubricato "conservazione della documentazione inerente alle segnalazioni", stabilisce che le segnalazioni e la relativa documentazione "sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione [...]". In conseguenza di ciò, il ciclo di vita dei dati personali trattati in occasione di una segnalazione di *whistleblowing* ha inizio dalla data di ricevimento della segnalazione (è direttamente il *whistleblower* ad effettuare la comunicazione di dati personali, propri e delle persone coinvolte nella segnalazione) e terminerà decorsi 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione (termine massimo entro il quale il Titolare può conservare la segnalazione e la documentazione ad essa allegata); si veda l'art. 14, co. 1 d.lgs. 24/2023.

Risorse di supporto dei dati

Con riferimento alle segnalazioni effettuate mediante piattaforma informatica, *Whistleblowing Solutions Impresa Sociale S.r.l.* si avvale di *Seeweb S.R.L.*, qualificata come *sub*-responsabile del trattamento, per procedere all'archiviazione in cloud dei dati. I dati sono salvati con backup giornaliero incrementale su Data Center delocalizzato basato su Veeam Backup & Replication con 7 *restore point*. Tutti i datacenter dai quali sono erogati i servizi sono situati sul territorio italiano e posti ad elevata distanza, tale da assicurare la completa indipendenza dei domini di disastro secondo le normative internazionali. Tutti i datacenter sono di proprietà e in completa gestione del fornitore.

Finalità del trattamento

Le finalità del trattamento consistono nella gestione delle segnalazioni di *whistleblowing*, a prescindere dalla modalità con la quale sono pervenute all'Ente. Qualsiasi segnalazione, a meno che non si tratti di notizie palesemente prive di fondamento, di informazioni che sono già totalmente di dominio pubblico o di informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio), deve essere istruita dal RPCT al fine di accertare la veridicità di quanto segnalato. Nel caso dovesse risultare necessario, il RPCT potrà comunicare l'esito dell'accertamento all'ANAC, all'autorità giudiziaria o attivare il procedimento disciplinare nei confronti del segnalato o del segnalante.

Basi giuridiche del trattamento

I dati forniti vengono trattati per svolgere l'istruttoria della segnalazione e dar seguito alla stessa, ai sensi dell'art. 5 del d.lgs. 24/2023, allo scopo di accertare eventuali violazioni delle norme previste dal decreto *whistleblowing*. La base giuridica di tale trattamento è quindi rappresentata dall'art. 6, par. 1, lett. c) del Regolamento UE 2016/679 ("il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento").

Nei casi di cui all'art. 12, commi 3, 4 e 5 d.lgs. 24/2023, può presentarsi la necessità di rivelare l'identità della persona segnalante; nel caso previsto dal comma 5, per poter palesare l'identità del segnalante è necessario chiedere il consenso a quest'ultimo. In questo caso, pertanto, la base giuridica del trattamento è rappresentata dall'art. 6, par. 1, lett. a) del Regolamento UE 2016/679 ("l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"). L'Ente, nell'informativa messa a disposizione dell'interessato da evidenza che il mancato consenso a tale rivelazione comporterà, in ambito

disciplinare, l'inutilizzabilità della segnalazione, ponendo fine al procedimento in corso; in secondo luogo, l'Ente ricorda che, ai sensi dell'art. 7, par. 3, Regolamento UE 2016/679, "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca."

I dati sono adeguati, pertinenti e limitati

I dati sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. La normativa di riferimento e le linee guida ANAC chiariscono che le violazioni segnalate devono essere circostanziate il più possibile per consentire un'agevole verifica e analisi dei fatti descritti nella segnalazione.

I dati sono esatti ed aggiornati

I dati sono esatti e, se necessario, aggiornati come previsto dall'art. 5 par. 1 lett. e) del Regolamento UE 2016/679. Anche nel caso in cui la segnalazione dovesse pervenire per mezzo della piattaforma elettronica adottata dall'Ente, il *whistleblower*, grazie al *key code* generato all'esito della procedura di segnalazione, ha sempre la possibilità di aggiornare i dati ed il contenuto della segnalazione.

Periodo di conservazione dei dati

Come previsto dall'art. 13 del d.lgs. n. 24 del 10 marzo 2023, le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione nel rispetto degli obblighi di cui all'art. 12 del d.lgs. 10 marzo 2023 n. 24 e del principio di cui agli articoli 5 par. 1 lett. e) del Reg. UE 2016/679.

Informativa e consenso

Viene resa apposita informativa ex art. 13 Reg. UE 2016/679. Questa è pubblicata sul sito istituzionale dell'Ente e, inoltre, viene consegnata in versione cartacea nell'ipotesi in cui il *whistleblower* richieda l'incontro diretto con il RPCT.

Considerata l'ipotesi disciplinata dall'art. 12, co. 5 d.lgs. 24/2023, nell'informativa messa a disposizione dell'interessato l'Ente da evidenza che il mancato consenso alla rivelazione dell'identità del segnalante comporterà, in ambito disciplinare, l'inutilizzabilità della segnalazione, ponendo fine al procedimento in corso; in secondo luogo, l'Ente ricorda che, ai sensi dell'art. 7, par. 3, Regolamento UE 2016/679, "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca."

Responsabili del trattamento

Viene individuato quale Responsabile del trattamento la Società *Whistleblowing Solutions S.I. S.R.L.* che fornisce la piattaforma informatica per la gestione delle segnalazioni; come sub-responsabili del trattamento viene individuata Seeweb S.R.L., nominata da *Whistleblowing Solutions S.I. S.R.L. e Transparency International Italia*, nominato "per la collaborazione nella gestione del sistema di *whistleblowing*".

Il fornitore è stato nominato quale responsabile del trattamento ai sensi degli artt. 4, n. 8) e 28 del Regolamento (UE) 2016/679 con un apposito accordo di nomina sottoscritto il 12/04/2023.

Destinatari di paesi terzi

I dati non vengono trasferiti in Paesi terzi.

VALUTAZIONE D'IMPATTO

- **Danno**

Definiamo il danno come l'effetto negativo determinato dal verificarsi degli effetti scaturiti da una minaccia. Il danno è causato dalla compromissione del dato personale dell'interessato in una o più delle tre dimensioni (riservatezza, disponibilità, integrità).

Legenda:

	DANNO	DESCRIZIONE
1	BASSO	Gli interessati possono incontrare alcuni piccoli inconvenienti, che potranno superare senza problemi (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
2	MEDIO	Gli interessati possono incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
3	ALTO	Gli interessati possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituzioni finanziaria, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4	CRITICO	Gli interessati possono incontrare conseguenze significative, o addirittura irreversibili, che loro non riescono a superare (incapacità al lavoro, disturbi psicologici o fisici di lungo termine, morte, ecc.).

- **Probabilità**

Definiamo probabilità la valutazione della frequenza o della possibilità che una determinata minaccia si concretizzi, in relazione al contesto esistente.

Legenda:

	PROBABILITA'	DESCRIZIONE
1	IMPROBABILE	Il verificarsi della minaccia richiederebbe la concomitanza di più eventi poco probabili. Non si sono quasi mai verificati fatti analoghi e il suo verificarsi susciterebbe incredulità.
2	POCO PROBABILE	Il verificarsi della minaccia richiederebbe circostanze non comuni e di bassa probabilità. Si sono verificati pochi fatti analoghi e il suo verificarsi susciterebbe sorpresa.
3	FREQUENTE	Si sono verificati altri fatti analoghi con una discreta frequenza tanto che il verificarsi della minaccia susciterebbe una modesta sorpresa.
4	RICORSIVO	Si sono verificati altri fatti analoghi e il verificarsi della minaccia è praticamente dato per scontato.

DISPONIBILITÀ - DANNI FISICI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): BASSO

- Probabilità di avverarsi dell'evento (rischio): IMPROBABILE

DISPONIBILITÀ - DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (impatto): BASSO

- Probabilità di avverarsi dell'evento (rischio): IMPROBABILE

DISPONIBILITÀ - DANNI IMMATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): MEDIO

- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

INTEGRITÀ - DANNI FISICI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): BASSO

- Probabilità di avverarsi dell'evento (rischio): IMPROBABILE

INTEGRITÀ - DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (Impatto): BASSO

- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

INTEGRITÀ - DANNI IMMATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): MEDIO

- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

RISERVATEZZA - DANNI FISICI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): BASSO

- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

RISERVATEZZA - DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (Impatto): MEDIO

- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

RISERVATEZZA - DANNI IMMATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): ALTO

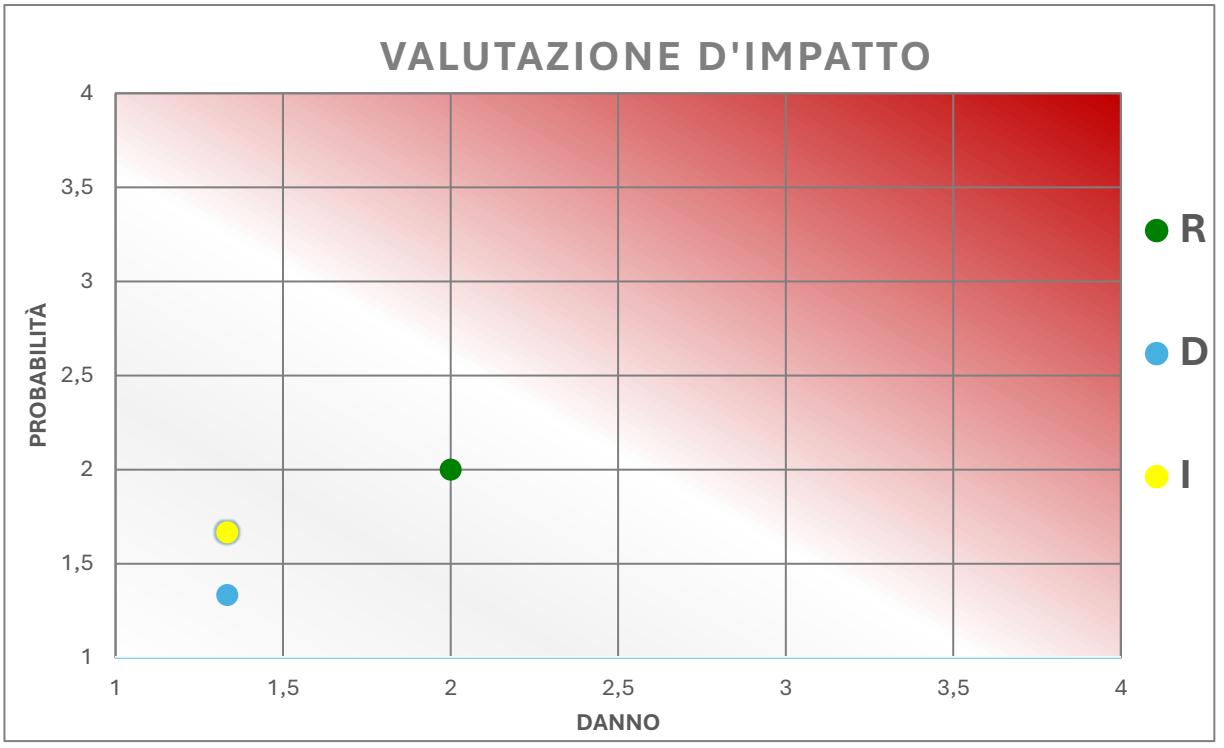
- Probabilità di avverarsi dell'evento (rischio): POCO PROBABILE

Comune di Portobuffolé

Provincia di Treviso

MAPPATURA DEL RISCHIO

Nel grafico sottostante è riportato il valore dell'impatto sui diritti e le libertà dell'interessato a cui appartengono i dati personali trattati dall'Ente durante le attività di trattamento sottoposte ad analisi.



Legenda:

R = riservatezza
D = disponibilità
I = integrità

} caratteristiche del dato personale

CONCLUSIONI

Considerate le risultanze della presente valutazione d'impatto e, nello specifico, un impatto per i diritti e le libertà degli interessati al di sotto del livello «alto» (per tutte le dimensioni del dato che potrebbero essere compromesse durante il trattamento), il Comune di Portobuffolè – allo stato attuale - non ritiene necessario attivarsi per predisporre un piano per il trattamento del rischio, in quanto ritiene che i rischi, seppur presenti, siano pienamente accettabili.

Documenti allegati:

- Disciplinare Whistleblowing (D.Lgs. 24/2023).

LUCA
SOCCORSO
03.03.2026
09:57:18
GMT+01:00