COMUNE DI CALDIERO

LINEE GUIDA SULLA VALUTAZIONE D'IMPATTO SUL TRATTAMENTO DEI DATI

(DPIA)

Art. 35 regolamento Ue 679/2016

Sommario

SCOPO DEL DOCUMENTO

Lo scopo del presente documento è fornire al personale comunale, ed in particolare agli Addetti al trattamento dei dati, le linee guida per l'elaborazione della Valutazione d'impatto sulla protezione dei dati // DPIA (*Data Protection Impact Assessment)*.

COS'E' LA DPIA

La DPIA è un processo finalizzato a valutare l'impatto sul diritto alla riservatezza ed alla protezione dei dati personali degli interessati[(1)].

PERCHE' VA FATTA LA DPIA

L'articolo 24 del Regolamento UE 679/2016, d'ora in poi GDPR, stabilisce che "*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.*

La DPIA serve quindi a dimostrare che il titolare del trattamento ha valutato i rischi connessi al trattamento e che ha attuato tutte le misure ritenute idonee a minimizzare i rischi.

QUANDO VA FATTA LA DPIA (in termini temporali)

La DPIA va effettuata prima dell'inizio del trattamento o, nel caso di trattamenti esistenti, se si ritiene che ci siano stati cambiamenti che impattano significativamente sulla gestione del trattamento (ad esempio *cambio di tecnologie*).

I SOGGETTI COINVOLTI

Il processo di valutazione d'impatto è *"imputabile"* al Titolare del trattamento, il quale opera con l'assistenza, la collaborazione ed il supporto dei seguenti soggetti /ruoli

Ruolo	Attività
Responsabile dell'unità organizzativa che gestisce il trattamento oggetto di	• Effettua la preventiva valutazione se il trattamento va soggetto a DPIA oppure no • In caso negativo provvede esclusivamente ad aggiornare o chiedere l'aggiornamento del registro

[1] Interessato è la persona fisica a cui si riferiscono i dati del trattamento

Ruolo	Attività
DPIA	dei trattamenti • In caso positivo attiva il processo di DPIA coinvolgendo il RTD
RTD (Responsabile transizione digitale)	• Prende in carico il procedimento ed avvia il procedimento di DPIA coinvolgendo i ruoli aziendali sotto indicati
Responsabile CED / Amministratori di sistema interni o esterni	• Fornisce supporto tecnico informatico nel processo di valutazione: individua le possibili minacce di tipo tecnologico; suggerisce le possibili azioni correttive per ridurre il rischio derivante dalle minacce; etc.
DPO (Data protection officier) / RPD (Responsabile protezione dei dati)	• Sovrintende e fornisce supporto al processo di valutazione
Esperti esterni	• Sono coinvolti nel caso in cui il processo di valutazione sia particolarmente complesso e necessiti di supporti specialistici (come ad esempio in caso di tecnologie innovative non sperimentate, particolarmente complesse o particolarmente invasive)
Fornitore degli strumenti tecnologici per la gestione del trattamento	• Nel caso il trattamento sia incentrato prevalentemente o completamente sull'utilizzo di tecnologie e/o strumenti / supporti tecnologici, la DPIA può essere richiesta al fornitore. In questo caso il processo di DPIA interno (la valutazione d'impatto del titolare) può riprendere ed utilizzare la DPIA effettuata dal fornitore.

QUANDO E' OBBLIGATORIA LA DPIA

Il processo di valutazione d'impatto non è sempre obbligatorio.

L'articolo 35 del GDPR (*General Data Protection Regulation*), stabilisce che "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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 10;*

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

L'Autorità di controllo italiana [Garante della Protezione dei Dati Personali, d'ora in poi GPDP o semplicemente Garante], anche sulla base delle indicazioni del WP 29 [Gruppo di Lavoro *"Articolo 29"* ora *European Data Protection Board – EDPB*] espresse nel documento WP 248 rev01 (*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), con provvedimento n. 467 dell'11 ottobre 2018, doc. web n. 9058979 ha individuato i casi in cui è obbligatoria la DPIA che si riportano di seguito:

Tabella 1 (trattamenti per i quali è obbligatoria la DPIA)

TRATTAMENTI SOGGETTI A DPIA OBBLIGATORIA
1. Trattamenti valutativi o di *scoring* su ***larga scala*** [2], nonché trattamenti che comportano la ***profilazione***[3] degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"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*".
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "*effetti giuridici*" oppure che incidono "*in modo analogo significativamente*" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un ***utilizzo sistematico*** [4] di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai 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, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un ***controllo a distanza*** dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti ***non occasionali*** di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

[2] Il GDPR non definisce la nozione di "***larga scala***", tuttavia fornisce un orientamento in merito al considerando 91. Ad ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati di seguito al fine di stabilire se un trattamento sia effettuato su larga scala:

e) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
f) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
g) la durata, ovvero la persistenza, dell'attività di trattamento;
h) la portata geografica dell'attività di trattamento.

[3] L'art. 4 del GDPR definisce **profilazione** *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"*.

[4] L'aggettivo *"**sistematico**"* ha almeno uno dei seguenti significati a giudizio del WP 29:

a) che avviene per sistema;
b) predeterminato, organizzato o metodico;
c) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
d) svolto nell'ambito di una strategia.

TRATTAMENTI SOGGETTI A DPIA OBBLIGATORIA
7. 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*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. 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*).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

QUANDO LA DPIA NON È OBBLIGATORIA

Secondo le Linee guida del Gruppo Art. 29, la DPIA non è obbligatoria per i trattamenti che:

a) non presentano rischio elevato per diritti e libertà delle persone fisiche;

b) hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;

c) sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;

d) sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;

e) fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

PERCHÉ E' OPPORTUNO EFFETTUARE SEMPRE LA DPIA

L'articolo 35 del GDR nella definizione dei casi in cui è obbligatoria la DPIA utilizza il termine "*in particolare*". Ciò significa che nei casi indicati la DPIA è sicuramente obbligatoria, ma rimane nella "responsabilità" del titolare del trattamento effettuare la DPIA laddove esistano dubbi sull'impatto che il

trattamento può avere sull'interessato. Il Garante ed il WP 29 (ora EDPB), infatti, nei casi dubbi, suggeriscono di effettuarla anche ai fini *dell'accountability*.

Al fine di **attirare l'attenzione dell'operatore sui rischi (RID) del trattamento ed al fine di dimostrare che sono stati effettivamente valutati i rischi connessi al trattamento i preposti al trattamento devono sempre effettuare sempre la DPIA in modo da dimostrare di aver valutato l'impatto del trattamento in ragione della protezione dei dati.**

CONTENUTI DELLA DPIA

L'articolo 35 del GDPR stabilisce che la DPIA deve contenere almeno:

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 di cui al paragrafo 1;*
d) *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*.

A fine di agevolare l'elaborazione del documento e di rendere omogeneo il processo di elaborazione della valutazione d'impatto nel Comune di Caldiero si forniscono le seguenti indicazioni sul contenuto del documento.

La DPIA deve prendere in considerazione i seguenti aspetti:

a) progetto: descrizione;
b) finalità del trattamento;
c) base giuridica che legittima il trattamento;
d) ambito del trattamento;
e) dati trattati;

f) *asset* utilizzati per il trattamento;

g) diritti degli interessati (*compreso la trasparenza)*;

h) valutazione del rischio;

i) esito della valutazione.

Descrizione del progetto e/o del trattamento che si intende realizzare

Spiegare a grandi linee il progetto: quale scopo si propone di raggiungere e che tipo di elaborazione comporta. Potrebbe essere utile fare riferimento o collegarsi ad altri documenti, come una proposta di progetto.

Finalità del trattamento

Indicare la finalità del trattamento. La finalità del trattamento è una risposta alla domanda "perché effettuo questo trattamento".

Base giuridica che legittima il trattamento

Indicare la base giuridica che legittima il trattamento [5]. Se la base giuridica è *l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento* è necessario siano indicati i relativi riferimenti normativi che attribuiscono o impongono al titolare quel determinato trattamento.

Ambito del trattamento

Al fine di individuare la "portata" del trattamento, e quindi, ad esempio, se si tratta di *"larga scala"* indicare:

a) la quantità di persone interessate;

---

[5] Le basi giuridiche che legittimano il trattamento sono stabilite dall'articolo 6 del GDPR che si riporta di seguito
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

b) l'area geografica coperta;

c) la durata del progetto / trattamento.

Dati

Qualità e quantità di dati raccolti classificati per tipologia.

Indicare i dati che si intendono raccogliere (a titolo esemplificativo).

Dati comuni

- ○ *Anagrafici (specificare)*
- ○ *estremi di documenti di identificazione*
- ○ *numeri di telefono privati*
- ○ *Indirizzo IP*
- ○ *E-mail*
- ○ *Dati bancari*
- ○ *Carte di credito*
- ○ *Codice fiscale*
- ○ *Dati sulle prestazioni*
- ○ *Immagini: foto, video, etc.*

Dati sanitari

- ○ *Gruppo sanguigno*
- ○ *Malattie*
- ○ *Green pass*
- ○ *Infortuni sul lavoro, registrazione della malattia, test antidroga/alcolici, valutazione a 365 gradi, test della personalità, disabilità*

Dati giudiziari

- ○ *Casellario giudiziario*
- ○ *Precedenti penali*

Dati biometrici

- ○ *Dati genetici*
- ○ *Registrazione voce*
- ○ *Impronte digitali o oculari*

Dati particolari

- ○ *Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica*
- ○ *Opinioni politiche*
- ○ *Origine razziale o etnica*
- ○ *Credenze religiose o filosofiche*
- ○ *Adesione sindacale*

Giustificazione della qualità e quantità di dati raccolti in rapporto alla finalità che si vuole conseguire

L'articolo 5 comma 1 lettera c) del GDPR stabilisce che quando si effettua un trattamento i dati trattati (raccolti ed elaborati) devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (*principio della «minimizzazione dei dati»*). È pertanto necessario giustificare se i dati trattati in rapporto alla finalità del trattamento rispettano il principio della proporzionalità e della minimizzazione

Condivisione dei dati

Indicare chi hanno come destinatari [6] i dati, se vengono condivisi con responsabili di trattamento [7] (esterni) e/o con soggetti terzi [8].

Conservazione dei dati

L'articolo 5 del GDPR stabilisce che i dati sono *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)*

Indicare quindi:

a) le modalità di conservazione dei dati [9]: (i) digitali, (ii) cartacee, (ii) dove sono conservati;

b) tempi di conservazione.

Trasferimento dati *extra* UE

Il GDPR dedica l'intero capo V) al trasferimento dei dati extra UE e ne disciplina le condizioni.

Indicare se i dati sono conservati all'interno della UE o extra UE[10].

Asset utilizzati per il trattamento

Gli asset sono gli strumenti utilizzati per effettuare il trattamento. Indicare gli asset utilizzati per effettuare il trattamento o i trattamenti oggetto di valutazione: (i) *hardware; (ii) software; (iii) strumenti cartacei; (iv) reti;* (v) *persone, etc.*

---

[6] Destinatario del dato è colui il quale riceve la comunicazione. Può essere un soggetto interno, esterno o un terzo.

[7] Responsabile (esterno) di trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 5 par. 1 punto 8 GDPR)

[8] Terzi sono tutti coloro che non siano titolari del trattamento, designati al trattamento o responsabili di trattamento.

[9] Si tenga presente che le pubbliche amministrazioni hanno l'obbligo di formare e conservare i documenti in formato digitale (art. 40 CAD; Linee guida AGID documento informatico)

[10] Anche la gestione dei dati in *cloud* comporta trasferimento dei dati per cui va valutato dove sono ubicati i server che contengono i dati.
La pubblicazione di dati su un sito web europeo non costituisce flusso di dati transfrontaliero (Corte di Giustizia Europea).

Considerazioni sulla tecnologia utilizzata

Descrivere al tecnologia utilizzata e commentare: (i) se è una tecnologia già sperimentata e collaudata; (ii) se è una tecnologia sperimentale; (iii) se la tecnologia che s'intende utilizzare ha creato problemi in passato; (iv) altro.

Diritti degli interessati

I diritti degli interessati sono stabiliti dagli articoli 15 e segg. del GDPR. Indicare come si intendono garantire:

- diritto alla trasparenza ed informazione sul trattamento dei dati (informative art. 13)
- diritto di accesso e portabilità dei dati (articoli 15 e 20);
- diritto di rettifica ed cancellazione (articoli 16, 17 e 19);
- diritto di opposizione e limitazione di trattamento (articoli 18, 19 e 21).

In questa sezione si deve indicare come si intendono garantire i diritti degli interessati, in particolare le modalità di diffusione dell'informativa e l'eventuale pubblicazione dell'esito della valutazione d'impatto.

LA VALUTAZIONE DEL RISCHIO

Definizione di rischio

Il rischio è un concetto probabilistico, è cioè la probabilità che accada un certo evento capace di causare un danno alle persone. La nozione di rischio implica l'esistenza di una sorgente di pericolo e delle possibilità che essa si trasformi in un danno.

Il rischio nell'ambito della protezione dei dati

Nell'ambito della protezione dei dati il rischio è il pericolo della "violazione dei dati" [rischio **RID**] e cioè:

a) violazione della **R**iservatezza dei dati

b) violazione dell'**I**ntegrità dei dati

c) violazione della **D**isponibilità dei dati

La valutazione

La valutazione del rischio va effettuata valutando:

a) la **probabilità di accadimento** (ambito probabilistico)

b) **l'impatto dell'evento** in caso di accadimento (danno che può provocare l'evento sui diritti e libertà degli interessati)

La matrice del livello di rischio

Dalla combinazione dei due fattori (*probabilità * impatto*), posizionati su una scala di valutazione, si ricava il livello di rischio.

Probabilità di accadimento

La probabilità di accadimento (del danno) si valuta individuando le possibili minacce e le misure di sicurezza adottate, valutando la possibilità di accadimento del danno nel caso di verifichi la minaccia.

Parametro	Declinazione	Valutazione
Molto improbabile	Il danno dipenderebbe da un concatenamento di eventi indipendenti; secondo gli addetti è impossibile il suo verificarsi oppure non è mai accaduto un danno simile	1
Poco probabile	Il danno dipenderebbe da condizioni sfavorevoli; eventi accaduti raramente	2
Probabile	Il danno dipenderebbe da condizioni non del tutto connesse alla situazione ma possibili; eventi già riscontrati in letteratura	3
Molto probabile	Il danno dipenderebbe da condizioni connesse alla situazione; eventi già accaduti	4

Impatto

L'impatto dell'evento si calcola tenendo presente le conseguenze che provoca la violazione a carico dell'interessato.

Parametro	Declinazione	Valutazione
Basso	I soggetti interessati possono andare incontro a disagi minori, facilmente superabili	1
Medio	I soggetti interessati possono andare incontro a conseguenze moderate, che dovrebbero essere in grado di superare anche se con probabili difficoltà	2
Alto	I soggetti interessati possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	3
Molto Alto	I soggetti interessati possono subire danni irreversibili, che non sono in grado di superare	4

La matrice del livello di rischio

La matrice di valori può essere articolata in base a necessità, ma si ritiene che in questa fase di prima applicazione della valutazione del rischio la matrice possa essere articolata su **quattro** livelli

Fig. 1 matrice livello di rischio

IMPATTO	**Altissimo**	4	8	12	16
	Alto	3	6	9	12
	Medio	2	4	6	8
	Basso	1	2	3	4
		Molto improbabile	**Poco probabile**	**Probabile**	**Molto probabile**
		PROBABILITA DI ACCADIMENTO			

Determinazione del rischio accettabile

Posto che non è possibile annullare completamente il rischio si potranno verificare le seguenti situazioni:

Valori < 6	Rischio accettabile e nessun intervento necessario
Valori da 6 a 9	Opportuna integrazione delle misure di sicurezza
Valori > 9	Necessaria integrazione delle misure di sicurezza

Esito della valutazione

La valutazione si conclude con un responso di esito e quindi:

(i) rischio accettabile > il trattamento può essere effettuato;

(ii) rischio elevato > invio di richiesta al garante ai sensi dell'articolo 36 del GDPR.

La probabilità di accadimento

Per calcolare la probabilità di accadimento del danno si sottopone a valutazione il trattamento:

(i) individuando le possibili minacce (per quel tipo di trattamento);

(ii) valutando le misure di sicurezza adottate (per quel trattamento);

(iii) valutando la probabilità che si verifichi il danno attribuendo alla probabilità un valore in base alla scala adottata, nel nostro caso da 1 a 4.

Il livello di rischio (probabilità di accadimento del danno) sarà dato da : (a) la media dei valori attribuiti alle diverse tipologie di danno; (b) le medie di ogni minaccia vanno sommate; (c) il totale va diviso per il numero di minacce valutate

Quindi, incendio: valutate le misure di sicurezza adottate si attribuisce un punteggio da 1 a 4 ai potenziali danni alla riservatezza, dove 1 la probabilità è molto improbabile e 4 è invece probabile. Esempio: (i) riservatezza = 1; (ii) integrità = 3; (iii) disponibilità = 3. Quindi 1+3+3 = 7, che diviso 3 è = a 2,3. Quindi poco probabile che si verifichi il danno

La valutazione va effettuata per ogni minaccia.

Per agevolare il lavoro è stato elaborato il seguente set di minacce:

ID	AMBITO	MINACCIA	MISURE DI SICUREZZA ADOTTATE	danni alla RISERVATEZZA	danni alla INTEGRITÀ	danni alla DISPONIBILITÀ	MEDIA
1	Danni fisici	Incendio		1 > 4	1 > 4	1 > 4	xxxx
2	Danni fisici	Allagamento					
3	Danni fisici	Polvere, corrosione, congelamento.					
4	Danni fisici	Distruzione di strumentazione da parte di persone malintenzionate					
5	Danni fisici	Attacchi (bombe, terroristi)					
6	Danni fisici	Fulmini e scariche atmosferiche					
7	Eventi naturali	Fenomeni climatici (Uragani, Nevicate)					
8	Eventi naturali	Terremoti, eruzioni vulcaniche					
9	Perdita di servizi essenziali	Guasto aria condizionata o sistemi di raffreddamento					
10	Perdita di servizi essenziali	Perdita di energia (o sbalzi di tensione)					
11	Perdita di servizi essenziali	Malfunzionamento nei componenti di rete					
12	Perdita di servizi essenziali	Errori di trasmissione (incluso il *misrouting*)					
14	Perdita di servizi essenziali	Interruzione di servizi erogati riconducibili ai fornitori esterni (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio, a causa di fallimento, chiusura, incidenti.					
15	Perdita di servizi essenziali	Indisponibilità del personale (malattie, sciopero, ecc.)					
16	Perdita di servizi essenziali	Perdita di fornitori, fallimento, incidenti					
17	Perdita di servizi essenziali	Errori dei componenti TLC					
18	Perdita di servizi essenziali	Danni alle linee TLC					
19	Perdita di servizi essenziali	Eccesso di traffico sulle linee TLC					
20	Disturbi	Disturbi elettromagnetici					
21	Compromissione di informazioni	Intercettazione (inclusa analisi del traffico)					
22	Compromissione di informazioni	Furto di documenti o supporti di memorizzazione					
23	Compromissione di informazioni	Furto di apparati o componenti					
24	Compromissione di informazioni	Recupero di informazioni da media (principalmente memorie di massa) dismessi.					
25	Compromissione di informazioni	Rivelazione di informazioni (da parte del personale o fornitori)					
26	Compromissione di informazioni	Infiltrazione nelle comunicazioni					
27	Compromissione di informazioni	Ricezione dati da origini non affidabili					
28	Compromissione di informazioni	Ripudio dei messaggi					

ID	AMBITO	MINACCIA	MISURE DI SICUREZZA ADOTTATE	danni alla RISERVATEZZA	danni alla INTEGRITÀ	danni alla DISPONIBILITÀ	MEDIA
29	Problemi tecnici	Fault o malfunzionamento della strumentazione IT					
30	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per i clienti					
31	Problemi tecnici	Malfunzionamenti pacchetti software usati internamente					
32	Problemi tecnici	Malfunzionamenti software applicativi sviluppati per uso interno					
33	Problemi tecnici	Errori di manutenzione hardware e software di base					
34	Problemi tecnici	Saturazioni dei sistemi IT					
35	Azioni non autorizzate	Uso non autorizzato della strumentazione					
36	Azioni non autorizzate	Alterazione volontaria e non autorizzata di dati di business					
37	Azioni non autorizzate	Virus (*malware*)					
38	Azioni non autorizzate	Accesso non autorizzato alla rete					
39	Azioni non autorizzate	Uso non autorizzato della rete da parte degli utenti					
40	Azioni non autorizzate	Trattamento (volontario o inconsapevole) non consentito di dati (personali)					
41	Azioni non autorizzate	Importazione o esportazione illegale di software (copia illegale di software o uso di software legale)					
42	Compromissione di funzioni	Errori degli utenti di business					
43	Compromissione di funzioni	Uso dei servizi da parte di persone non autorizzate					
44	Compromissione di funzioni	Degrado dei media (memorie di massa)					
45	Compromissione di funzioni	Uso di servizi in modo non autorizzato					
46	Compromissione di funzioni	Furto identità					

Per quanto riguarda le misure di sicurezza sono state individuate le seguenti misure di sicurezza che possono essere adottate:

ID CONTROMISURA	CONTROMISURA
1	*Backup* locale
2	*Backup* remoto
3	Impianto d'allarme
4	Sorveglianza perimetrale
5	Videosorveglianza
6	Parafulmine
7	Impianto antincendio
8	Porte con serratura
9	Inferriate alle finestre
10	Armadi ignifughi
11	Armadi blindati
12	Armadi con serratura
13	Armadi *rack*
14	Cassettiere
15	Copertura UPS
16	Cassaforte
17	Aria condizionata
19	Misura minima AGID ICT 1.1.1 ABSC

ID CONTROMISURA	CONTROMISURA
20	Misura minima AGID ICT 1.3.1 ABSC
21	Misura minima AGID ICT 1.4.1 ABSC
22	Misura minima AGID ICT 2.1.1 ABSC
23	Misura minima AGID ICT 2.3.1 ABSC
24	Misura minima AGID ICT 3.1.1 ABSC
25	Misura minima AGID ICT 3.2.1 ABSC
26	Misura minima AGID ICT 3.2.2 ABSC
27	Misura minima AGID ICT 3.3.1 ABSC
28	Misura minima AGID ICT 3.4.1 ABSC
29	Misura minima AGID ICT 4.1.1 ABSC
30	Misura minima AGID ICT 4.4.1 ABSC
31	Misura minima AGID ICT 4.5.1 ABSC
32	Misura minima AGID ICT 4.5.2 ABSC
33	Misura minima AGID ICT 4.7.1 ABSC
34	Misura minima AGID ICT 4.8.1 ABSC
35	Misura minima AGID ICT 4.8.2 ABSC
36	Misura minima AGID ICT 5.1.1 ABSC
37	Misura minima AGID ICT 5.1.2 ABSC
38	Misura minima AGID ICT 5.2.1 ABSC
39	Misura minima AGID ICT 5.3.1 ABSC
40	Misura minima AGID ICT 5.7.1 ABSC
41	Misura minima AGID ICT 5.7.3 ABSC
42	Misura minima AGID ICT 5.7.4 ABSC
43	Misura minima AGID ICT 5.10.1 ABSC
44	Misura minima AGID ICT 5.10.2 ABSC
45	Misura minima AGID ICT 5.10.3 ABSC
46	Misura minima AGID ICT 5.11.1 ABSC
47	Misura minima AGID ICT 5.11.2 ABSC
48	Misura minima AGID ICT 8.1.1 ABSC
49	Misura minima AGID ICT 8.1.2 ABSC
50	Misura minima AGID ICT 8.3.1 ABSC
51	Misura minima AGID ICT 8.7.1 ABSC
52	Misura minima AGID ICT 8.7.2 ABSC
53	Misura minima AGID ICT 8.7.3 ABSC
54	Misura minima AGID ICT 8.7.4 ABSC
55	Misura minima AGID ICT 8.8.1 ABSC
56	Misura minima AGID ICT 8.9.1 ABSC
57	Misura minima AGID ICT 8.9.2 ABSC
58	Misura minima AGID ICT 8.9.3 ABSC
59	Misura minima AGID ICT 10.1.1 ABSC
60	Misura minima AGID ICT 10.3.1 ABSC
61	Misura minima AGID ICT 10.4.1 ABSC

ID CONTROMISURA	CONTROMISURA
62	Misura minima AGID ICT 13.1.1 ABSC
63	Misura minima AGID ICT 13.8.1 ABSC
65	Percorso *privacy compliance*
66	Percorso *privacy specialist*
67	Stabile antisismico
68	Impianto messa a terra
69	Certificazione di rete
70	Estintori
71	Certificazione del fornitore
72	Configurazione sicura dei sistemi
73	Istruzione per la gestione del *data breach*
74	Modulo per l'esercizio diritti in materia di protezione dei dati personali
75	Procedura per la gestione dei diritti degli interessati
76	Procedura per la gestione di una valutazione di impatto sulla protezione del dato personale
77	Regolamento per la protezione dell'informazione
78	Politica per la protezione del *cyberspace*
79	Formazione di base del personale
80	Procedura di risposta agli incidenti di sicurezza
81	Identificazione degli *asset*
82	Controllo accessi
83	Configurazione sicura dei sistemi
84	Uso appropriato dei privilegi di amministratore
85	Protezione perimetrale
86	Protezione da virus
87	*Backup* e *restore*
95	Obbligo informativa
96	Verifica della correttezza della responsabilità

L’impatto dell’evento

L’impatto dell’evento si calcola attribuendo un valore da 1 a 4 alle possibili conseguenze derivanti dall’evento accaduto, secondo la scala di valori di cui sopra.

L’esito della valutazione ed il rischio accettabile

La valutazione della probabilità di rischio e dell’impatto vanno inseriti nella matrice di rischio.

IMPATTO	**Altissimo**	4	8	12	16
	Alto	3	6	9	12
	Medio	2	4	6	8
	Basso	1	2	3	4
		Molto improbabile	**Poco probabile**	**Probabile**	**Molto probabile**
		PROBABILITA DI ACCADIMENTO			

In base al risultato si potrà avere

Valori < 6	Rischio accettabile e nessun intervento necessario
Valori da 6 a 9	Opportuna integrazione delle misure di sicurezza
Valori > 9	Necessaria integrazione delle misure di sicurezza, oppure rinuncia al trattamento o richiesta autorizzazione al GPDP ex art. 36 RGPD.

COMUNE DI CALDIERO

VALUTAZIONE D'IMPATTO

DPIA

Art. 35 Regolamento UE 679/2016

1. **Descrizione del progetto**

2. **Finalità del trattamento**

3. **Base giuridica che legittima il trattamento**

4. **Ambito del trattamento**

5. **Dati**

6. **Giustificazione della qualità e quantità di dati raccolti in rapporto alla finalità che si vuole conseguire**

7. **Condivisione dei dati**

8. **Conservazione dei dati**

9. **Trasferimento dati extra UE**

10. ***Asset* utilizzati per il trattamento**

11. **Considerazioni sulla tecnologia utilizzata**

12. **Misure di sicurezza adottate**

13. **Diritti degli interessati**

14. Valutazione del rischio

15. Matrice del livello di rischio

16. Determinazione del rischio accettabile

17. Esito della valutazione