



VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Azienda/Organizzazione

Comune di Arce

TITOLARE	
-----------------	--

SEDE	Palazzo Comunale ARCE
-------------	--------------------------

Data revisione: 01/03/2025

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui

andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- 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.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento (**C**). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze (C)** è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
Conseguenze						

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un **Livello di Rischio** (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA - valutazione del rischio normalizzato

Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevedono due o più criteri di obbligo DPIA.

Nel caso in cui, quindi, l'indice di rischio si colloca nel range $15 \div 25$, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

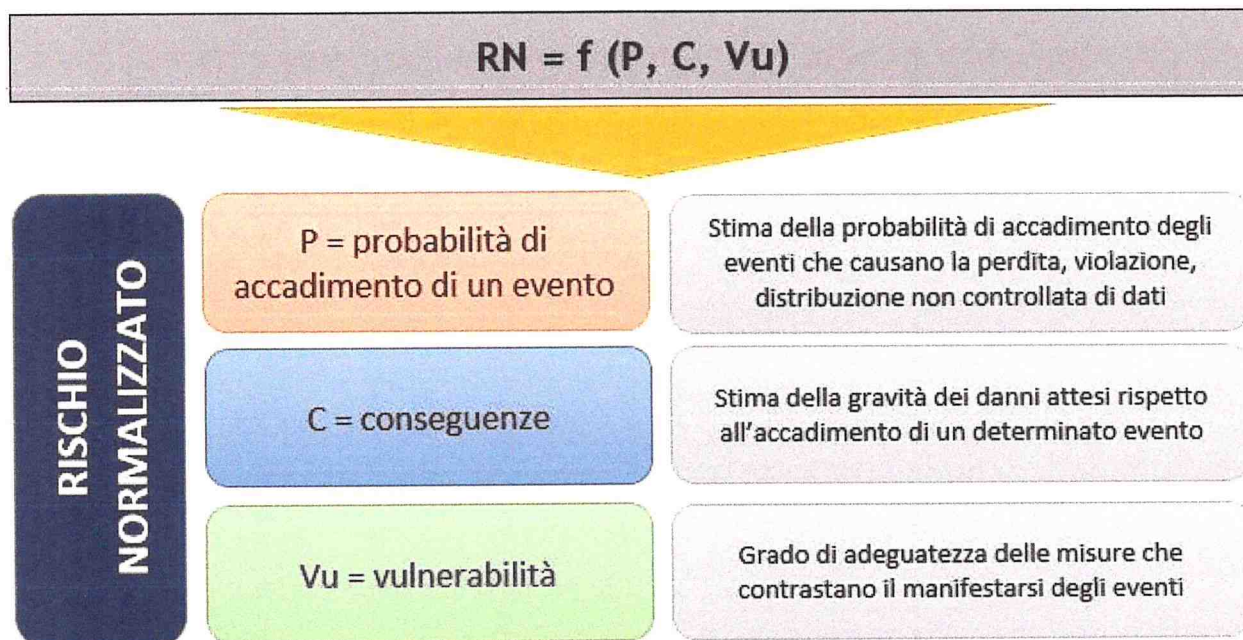
Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f (P, C, Vu)$$

Dove:

P = probabilità

C = conseguenze generate dall'evento



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco R_i come prodotto della probabilità P e delle conseguenze C , in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

P R O B A B I L I T À	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	(1 ≤ Ri ≤ 2)
Basso	(3 ≤ Ri ≤ 4)
Rilevante	(6 ≤ Ri ≤ 9)
Elevato	(12 ≤ Ri ≤ 16)

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Elevato	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Enti pubblici - Registro Responsabile dati - Polizia Locale - Responsabile del trattamento
- Videosorveglianza - Registro Responsabile dati - Polizia Locale - Responsabile del trattamento

Enti pubblici - Registro Responsabile dati - Polizia Locale - Responsabile del trattamento

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede operativa
Personale coinvolto	
Responsabile del trattamento	Pescosolido Manuela Dott.ssa Pescosolido Manuela, c.f. ██████████ <ul style="list-style-type: none"> • Blocco • Cancellazione • Comunicazione • Conservazione • Consultazione • Diffusione • Distribuzione • Elaborazione • Interconnessione • Modifica • Organizzazione • Raccolta • Raffronto
Persone autorizzate	TOTO FABIO, c.f. ██████████ <ul style="list-style-type: none"> • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta • Raffronto BALZANO MARINA, c.f. ██████████ <ul style="list-style-type: none"> • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione

	<ul style="list-style-type: none"> • Raccolta • Raffronto
Partners - Responsabili esterni	
Altro	

Processo di trattamento	
Descrizione	Funzioni amministrative per il perseguimento di interessi pubblici
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	<p>Relazioni con il pubblico</p> <p>Amministrazione degli stranieri (rilascio di permessi, visti di riconoscimenti di titoli)</p> <p>Amministrazione della popolazione (anagrafe, registri dello stato civile)</p> <p>Pianificazione urbanistica, amministrazione del territorio, controllo su illeciti edilizi</p> <p>Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati)</p> <p>Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione</p> <p>Autorizzazioni, concessioni, permessi, licenze e nullaosta</p> <p>Attività istituzionale delle forze armate o per la difesa e la sicurezza dello Stato</p> <p>Amministrazione della giustizia (procedimenti giudiziari civili, penali, amministrativi e tributari)</p> <p>Adempimenti agli obblighi di legge</p> <p>Compilazione schede di notificazione</p> <p>Controllo accessi</p> <p>Raccolta di dati e informazioni al fine di tutelare la sicurezza per prevenire o smascherare frodi</p> <p>Rilevazione, prevenzione e controllo delle infrazioni</p> <p>Servizi di controllo interno (della sicurezza, della produttività, della qualità dei servizi, dell'integrità patrimonio)</p>
Tipo di dati personali	<p>Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)</p> <p>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)</p> <p>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)</p> <p>Particolari (sensibili)</p> <p>Personali</p>
Categorie di interessati	<p>Enti</p> <p>Soggetti o organismi pubblici</p> <p>Clienti ed utenti</p> <p>Dipendenti</p>
Categorie di destinatari	<p>Soggetti che svolgono attività di archiviazione della documentazione</p> <p>Diffusione al pubblico</p> <p>Clienti ed utenti</p> <p>Società e imprese</p> <p>Associazioni ed enti locali</p>
Informativa	Non necessaria
Profilazione	Non necessario

Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> - Sono definiti i ruoli e le responsabilità - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Sono definiti i ruoli e le responsabilità	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Sono utilizzati software	<ul style="list-style-type: none"> • Compromissione informazioni 	Adeguate

antivirus e anti intrusione	(intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata 		

<ul style="list-style-type: none"> • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

Videosorveglianza - Registro Responsabile dati - Polizia Locale - Responsabile del trattamento

Struttura	<ul style="list-style-type: none"> • Amministrazione • Sede legale • Sede operativa
Personale coinvolto	
Responsabile del trattamento	Pescosolido Manuela
Persone autorizzate	Dott.ssa Pescosolido Manuela, c.f. ██████████ <ul style="list-style-type: none"> • Blocco • Cancellazione • Comunicazione • Conservazione • Consultazione • Diffusione

	<ul style="list-style-type: none"> • Distribuzione • Elaborazione • Interconnessione • Modifica • Organizzazione • Raccolta • Raffronto <p>BALZANO MARINA, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Blocco • Cancellazione • Conservazione • Consultazione • Interconnessione • Organizzazione • Raccolta • Raffronto <p>TOTO FABIO, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Blocco • Cancellazione • Conservazione • Consultazione • Interconnessione • Organizzazione • Raccolta • Raffronto
<p>Partners - Responsabili esterni</p>	<p>ARCESE PAOLO, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Consultazione <p>HELLOTEL TELECOMUNICAZIONI SRL, p.iva [REDACTED], nella persona di CAPOGNA LOREDANA</p> <ul style="list-style-type: none"> • Consultazione <p>Ligori Luciano, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Consultazione <p>V. Com.te Martiniello Antonio, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Consultazione <p>MARANCI CRISTIANO, c.f. [REDACTED]</p> <ul style="list-style-type: none"> • Blocco • Organizzazione
<p>Altro</p>	

Processo di trattamento	
Descrizione	Sistemi di rilevazione delle immagini
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Interesse pubblico Salvaguardia degli interessi vitali
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Interesse pubblico Salvaguardia degli interessi vitali
Finalità del trattamento	Protezione e incolumità degli individui Protezione della proprietà Rilevazione, prevenzione e controllo delle infrazioni Acquisizione di prove

	Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione
Tipo di dati personali	Particolari (sensibili) Personal Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)
Categorie di interessati	Soggetti o organismi pubblici Dipendenti Clienti ed utenti
Categorie di destinatari	Autorità di vigilanza e controllo Uffici giudiziari Forze di polizia Datore di lavoro
Informativa	Si
Profilazione	Si
Dati particolari	Si
Consenso minori	Si
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Informatica

Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO

RISCHIO	PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Accesso dati non autorizzato	Poco probabile	Gravi	Rilevante
Distruzione non autorizzata	Poco probabile	Gravi	Rilevante
Divulgazione non autorizzata	Poco probabile	Gravi	Rilevante
Modifica non autorizzata	Poco probabile	Gravi	Rilevante
Perdita	Poco probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- Esistono procedure per l'individuazione del custode delle password
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e

cartacee

- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
E' applicata una gestione della password degli utenti	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
E' eseguita la DPIA	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso 	Adeguate

	non autorizzato di strumentazione, ecc.)	
Esistono procedure per l'individuazione del custode delle password	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
L'impianto elettrico è certificato ed a norma	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	<ul style="list-style-type: none"> • Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) 	Adeguate
Sono applicate regole per la gestione delle password.	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, 	Adeguate

	<p>ecc.)</p> <ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	
Sono definiti i ruoli e le responsabilità	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Sono utilizzati software antivirus e anti intrusione	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Viene eseguita opportuna manutenzione	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		

<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO

Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

Arce, 06-03-2025



Luigi Di Marco



Alfredo Pescosolido