Società è-comune s.r.l. Security Policy

La società è-comune s.r.l. (da qui in proseguo "Società") tutela e garantisce la riservatezza, l'integrità e l'accesso ai dati personali ai diretti interessati posseduti dalla Società.
Garantisce, inoltre, che tutte le innovazioni apportate dal Regolamento (UE) 2016/679, o GDPR *(General Data Protection Regulation*), riguardante il trattamento dei dati personali, sono state prese in carico, analizzate e applicate senza ritardo.
La Società garantisce misure organizzative e procedurali adeguate a soddisfare la sicurezza dell'Interessato e dei suoi dati personali, quali un Codice etico e di comportamento aziendale in ossequio all'art. 24 del GDPR, la formazione degli amministratori, dei dipendenti, dei soci e dei collaboratori e l'adozione di *Non-disclosure Agreement* (Accordo di non Divulgazione), al quale è soggetto tutto il personale.
Il trattamento dei dati posto in essere dalla Società è conforme in ogni sua parte al GDPR. Di seguito elenchiamo gli aspetti della *Security Policy* attuate.

Articolo 1 - Sistemi di sicurezza

Al fine di proteggere i dati personali in possesso della Società, questa si è dotato di efficaci sistemi di prevenzione contro indebite intrusioni o *data breach.*
I sistemi impiegati si differenziano in meccanici e informatici: i sistemi meccanici in uso si costituiscono in una solida porta d'ingresso rinforzata, unica via d'accesso ai locali ove avviene il trattamento. La Società utilizza solidi armadietti dotati di serratura le cui chiavi sono in uso unico del Titolare del trattamento e dei soggetti da quest'ultimo indicati per l'espletamento delle sue funzioni. Gli armadietti in uso presso la sede del trattamento sono adoperati esclusivamente per la custodia dei dati personali registrati su supporti cartacei o fisici di *storage* esterno, quali HDD, SSD e NAS.
I sistemi informatici impiegati si costituiscono in account personali protetti da password, gestione puntuale degli accessi al materiale condiviso su Google Drive e misure di sicurezza conformi al GDPR (https://cloud.google.com/security/gdpr/?hl=it); inoltre, viene utilizzato un dispositivo di storage esterno NAS dotato di protezione dei dati con tolleranza di errore di 1 disco. I terminali si trovano in una zona interdetta al pubblico e sono protetti con password.

Articolo 2 - Videosorveglianza

La Società si è dotata di un impianto di videosorveglianza al fine di meglio tutelare la sicurezza delle persone fisiche e l'integrità del patrimonio aziendale. Il trattamento ha come sua base giuridica il legittimo interesse del titolare.
In ossequio alla normativa vigente, il personale e gli utenti sono opportunamente informati tramite apposita cartellonistica che stanno per accedere a un'area sottoposta a videosorveglianza.
Qui di seguito si elenca la posizione precisa delle telecamere tuttora attive:

1) sulla parete posta alla destra della rampa di accesso all'ecocentro;
2) sulla facciata d'ingresso ai locali adibiti all'amministrazione;
3) sulla facciata posta alla sinistra dell'ingresso ai locali adibiti all'amministrazione;
4) sulla parete che si affaccia sul piazzale centrale.

Le immagini riprese sono visionate solo dal personale a ciò preposto e conservate per un periodo massimo non eccedente le 48 ore (quarantotto), al fine di accertare l'esistenza di una responsabilità per dolo o per colpa in caso di danni a cose e/o persone. Allo scadere del suddetto termine le registrazioni saranno irrimediabilmente distrutte, comprese le loro copie, salvo che le registrazioni siano necessarie alle Autorità per lo svolgimento delle attività inquirenti.
Il personale addetto alla videosorveglianza è detentore unico del codice di sicurezza necessario per avere accesso alle immagini riprese dalle telecamere, e si impegna, altresì, a non rivelare a terzi tale codice.
Il sistema di videosorveglianza, al fine di diminuire il rischio di indebite intrusioni o di diffusione delle immagini, non è collegato a reti informatiche (Internet).

Articolo 3 - Personale

Tutto il personale che svolge attività lavorative all'interno dell'organigramma della Società è approfonditamente istruito in merito ai trattamenti che può effettuare sui dati personali raccolti e in merito agli accessi che può effettuare nelle banche dati presenti nell'infrastruttura, ed è vincolato al silenzio per mezzo di idonei patti di riservatezza.
Il personale è altresì esaustivamente istruito sulle violazioni che, se poste in essere, avrebbero rilevanza in sede sia civile che penale, al fine di scoraggiare condotte illecite derivanti da trattamenti non consentiti.
Tutte le attività del personale (interno ed esterno) sono esplicitate in lettere di incarico personali opportunamente protocollate nel registro del trattamento.

Articolo 4 - Il Titolare del Trattamento dei dati Personali

Il Titolare del trattamento si impegna a non rivelare a terzi l'ubicazione degli armadietti di cui all'art. 1, né di informarli circa il loro contenuto.
Il Titolare del trattamento provvede all'adeguata custodia delle chiavi necessarie per effettuare l'accesso al contenuto degli armadietti e dei locali.
Il Titolare non rivela a soggetti terzi le password di accesso ai terminali di lavoro ove sono trattati i dati né l'ubicazione delle chiavi.
Il Titolare del trattamento dei dati personali tiene un'accurata rendicontazione dei dati raccolti e dei trattamenti effettuati sotto la propria responsabilità all'interno del registro delle attività di trattamento, e lo rende accessibile in qualsiasi momento e senza limitazione alcuna al Garante per la Protezione dei dati personali e a qualsiasi altra Pubblica Autorità che ne facesse espressa richiesta, in ottemperanza a un ordine legittimo da quest'ultima promanato.
Il Titolare del trattamento, inoltre, effettua un'opportuna valutazione circa i dati personali in suo possesso e i rischi derivanti dal trattamento di questi ultimi, tenendo costantemente aggiornati i sistemi di sicurezza al fine di impedire il verificarsi di violazioni o comunque di circoscrivere i danni che ne potrebbero derivare, adeguandoli in tempo reale per garantire un livello di sicurezza proporzionato ai rischi *ex* art. 32 GDPR.
In caso di nomina di un Responsabile del trattamento dei dati personali o di un Responsabile della Protezione dei Dati (RPD), il Titolare del trattamento si impegna a utilizzare i più stringenti criteri di valutazione, tenendo conto dei soli meriti della persona, del suo livello di istruzione, della sua professionalità, dell'esperienza maturata e delle concrete esigenze della Società, al fine di garantire un servizio di alta qualità circa il trattamento dei dati personali e la loro protezione.

Il Titolare del trattamento dei dati personali, su espressa richiesta dell'Interessato o comunque una volta conseguite le finalità per le quali i dati sono stati raccolti, procederà alla restituzione di tutti i dati in possesso della Società, alla loro definitiva cancellazione dai suoi apparati e alla distruzione fisica di tutti i supporti cartacei e di tutte le copie realizzate, senza ulteriore ritardo, salvo il caso in cui questi siano conservati ai fini statistici o di interesse pubblico. La Società, in tali casi, si accerta di attuare le politiche in grado di rispettare il principio di minimizzazione dei dati, quali la loro pseudonimizzazione, così come richiesto *ex* 89, paragrafo 1, GDPR, dimodoché vengano assicurati i diritti e le libertà degli interessati.

Articolo 5 - Valutazione d'impatto sulla protezione dei dati (DPIA)

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*" (art. 35 GDPR).
I dati in possesso della Società riguardano, oltre ai dati anagrafici, i rifiuti che gli interessati conferiscono nell'ecocentro.
Questi sono stati raccolti per ovvie ragioni: senza questi, la Società non sarebbe in grado di conseguire il suo oggetto sociale, ovverosia il corretto smistamento e smaltimento dei rifiuti conferiti dalla cittadinanza.
Ai sensi dell'art. 35, paragrafo 3, GDPR, 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, GDPR, 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.

5.1 Criteri

Nel percorso di analisi sono stati presi in considerazione i seguenti 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 a 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, si ritiene necessario eseguire una valutazione d'impatto sulla protezione dei dati.
Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità, al fine di tenerla costantemente aggiornata.

DESCRIZIONE DELL'ALGORITMO DI VALUTAZIONE ADOTTATO:

5.2 Identificazione dei trattamenti

Il primo passaggio consiste nel censire tutte le attività di trattamento di dati personali, specificando:

- 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.

5.3 Valutazione del rischio e individuazione criteri per DPIA: spiegazione dell'equazione utilizzata.

Il rischio è uno scenario che descrive un *data breach* 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 (indicata con la lettera P) e alle conseguenze di tale evento (indicata con la lettera C). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

dove "LR" sta per Livello del Rischio, "P" sta per Probabilità di accadimento e "C" sta per Conseguenze. Alla probabilità di accadimento dell'evento P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITÀ DELL'EVENTO

1	Improbabile
2	Poco probabile
3	Probabile
4	Molto 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

Il diagramma che scaturisce dalla combinazione di probabilità e conseguenze è rappresentato nella figura seguente:

Probabilità						
	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 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

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

Prendendo in esame i criteri individuati al punto 4.1, possiamo comprendere a quale livello di rischio ci troviamo: difatti, se vi è la presenza di almeno due criteri tra quelli sopracitati e/o il Livello di Rischio risulta Ato, l'attività richiede la DPIA.

5.4 DPIA e 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 l'indice di rischio si colloca nel range tra 15 e 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:

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

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 Ri 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 è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Dunque, possiamo avere questa tabella di riferimento:

PROBABILITÀ					
	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)*
Alto	*(12 ≤ Ri ≤ 16)*

Il Rischio Intrinseco viene ricavato prendendo in considerazione tutti i possibili rischi e pericoli.
Di seguito la suddivisione delle aree di pericolo con i rischi generati:

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	Perdita; Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	Perdita; Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti all'impianto di videosorveglianza, interruzione collegamenti di rete, ecc.)	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, ecc.)	Perdita; Distruzione non autorizzata; Modifica non autorizzata; Divulgazione non autorizzata; Accesso dati non autorizzato
Compromissione riservatezza dei dati custoditi (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Perdita; Distruzione non autorizzata; Modifica non autorizzata; Divulgazione non autorizzata; Accesso dati non autorizzato
Azioni non autorizzate (errori volontari o involontari, virus, malware, uso non autorizzato di strumentazione, ecc.)	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 (V) che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.
Alla Vulnerabilità (V) 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:
Per ricavare il valore del Rischio Normalizzato (indicato con le lettere "RN") viene moltiplicato il Rischio Intrinseco per il valore peggiore assegnato alle misure di sicurezza relativamente a quello specifico rischio.

V					
	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 V	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Nota bene: se, dall'esito dell'analisi, si evince che l'attività rimane nella fascia Alta, il Titolare è tenuto a consultare preventivamente il Garante.

5.5 Risultati DPIA È-Comune Srl

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.

Processo di trattamento	
Descrizione	Videosorveglianza
Fonte dei dati personali	Telecamere di sorveglianza
Base giuridica per il trattamento dei dati personali	Legittimo interesse del Titolare
Durata del trattamento	48 ore o per un periodo superiore nel caso in cui i dati siano necessari per l'accertamento di responsabilità per dolo o per colpa
Finalità del trattamento	Protezione e incolumità degli individui; tutela del patrimonio aziendale; accertamento di responsabilità in sede civile e/o penale; repressione dei reati

Tipo di dati personali	Immagini video ritraenti la persona degli utenti dell'ecocentro
Categorie di interessati	Adulti
Categorie di destinatari	Personale addetto ad attività di supervisione delle immagini e di archiviazione della documentazione ai fini della sicurezza delle persone e del patrimonio aziendale
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	No
Frequenza trattamento	Quotidiano
Termine cancellazione dati	Le registrazioni saranno conservate per massimo 48 ore (quarantotto) a decorrere dal momento della rilevazione dei dati
Trasferimento dati (Paesi terzi)	No
Autorizzazione del Garante	Non presente; Non necessaria

Modalità di elaborazione dati: Elettronica	
Strumenti	Software di riprese per telecamere di videosorveglianza
Strutture informatiche di archiviazione: HDD esterni e NAS	
Strutture informatiche di backup: HDD esterni NAS	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Limitate	Accettabile

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADOTTATE
- È eseguita la DPIA; - È presenta una politica per la sicurezza e la protezione dei dati; - Impianto elettrico dotato di misure salvavita atte a evitare cortocircuiti e possibili incendi; - L'impianto elettrico è certificato e a norma; - Sono definiti i ruoli e le responsabilità; - Sono utilizzati software antivirus e anti-intrusione; - Viene eseguita opportuna manutenzione; - Viene eseguita una regolare formazione del personale; - Presenza di solida porta d'ingresso rinforzata; - Armadi chiusi con chiavi in dotazioni uniche al Titolare; - Dispositivi di storage esterno presenti; - Il backup viene effettuato quotidianamente; - Nelle aree dove vengono stoccati i dati l'accesso è interdetto al pubblico.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

Le misure di sicurezza sono risultate essere adeguate alla tutela della riservatezza dei dati delle persone fisiche oggetto di trattamento presso la società È-Comune Srl.

VALUTAZIONE DEI RISCHI

PERICOLO
Agenti fisici (incendio, allagamento, attacchi esterni)
RISCHI
· Perdita · Distruzione non autorizzata

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Limitate	Basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - RI	Vulnerabilità - V	Rischio normalizzato - RN
Basso	0,5	Basso

PERICOLO
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)
RISCHI
· Perdita · Distruzione non autorizzata

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Limitate	Basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		

Rischio intrinseco - Ri	Vulnerabilità - V	Rischio normalizzato - RN
Basso	0,5	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
· Perdita · Distruzione non autorizzata · Modifica non autorizzata · Divulgazione non autorizzata · Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - RI
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - RI	Vulnerabilità - V	Rischio normalizzato - RN

Molto basso	0,5	Molto basso

PERICOLO		
Problemi tecnici (anomalie e malfunzionamento software, problemi hardware o componenti servizio IT, ecc.)		
RISCHI		
· Perdita · Distruzione non autorizzata · Modifica non autorizzata · Divulgazione non autorizzata · Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - RI	Vulnerabilità - V	Rischio normalizzato - RN
Molto basso	0,5	Molto basso

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
RISCHI
· 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 *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	Vulnerabilità - V	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (errori volontari o involontari, virus, malware, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
· Perdita · Distruzione non autorizzata · Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - RI	Vulnerabilità - V	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

Il risultato della DPIA mostra che l'attività ha un rischio complessivo Basso.

Articolo 6 - Procedure di emergenza

Nell'organigramma della Società è previsto che i soggetti coinvolti nelle attività di trattamento collaborino attivamente con il Titolare del trattamento al fine di coordinare tutte le operazioni atte a neutralizzare le minacce concrete o presunte ai dati personali oggetto di trattamento.
Nel caso in cui si riscontrasse una violazione, la Società provvederà ad avvertire senza ritardo l'Interessato e tutti gli altri soggetti i cui diritti e le cui libertà fondamentali possono subire un

pregiudizio da questa. Contestualmente a ciò, la Società provvederà a rendere nota la violazione anche alle autorità competenti, come il Garante per la protezione dei dati personali e le Forze dell'Ordine, affiancando questi ultimi nella fase inquirente per accertare la concretezza della violazione ed eventualmente stimarne l'entità.
La Società è dotata di un Manuale Operativo idoneo a guidare il personale nelle procedure di emergenza.
Nota bene: il Manuale Operativo NON sostituisce la figura professionale del DPO.

Articolo 7 – Privacy policy

La Società assicura la minimizzazione dei dati raccolti e la liceità dei suoi trattamenti.
Gli interessati vengono esaustivamente informati circa le finalità per le quali tali dati vengono raccolti, il luogo ove viene posto in essere il trattamento, i soggetti coinvolti nel trattamento medesimo, i diritti esercitabili, i soggetti ai quali possono rivolgersi in caso di violazione concreta o meramente presunta e le modalità per farlo tramite una privacy policy a disposizione del pubblico.

Per qualsiasi informazione o chiarimento in merito ai temi trattati, Vi invitiamo a contattare la società È-Comune Srl all'indirizzo PEC ecomune@pec.it

Addì,

In fede,

_____