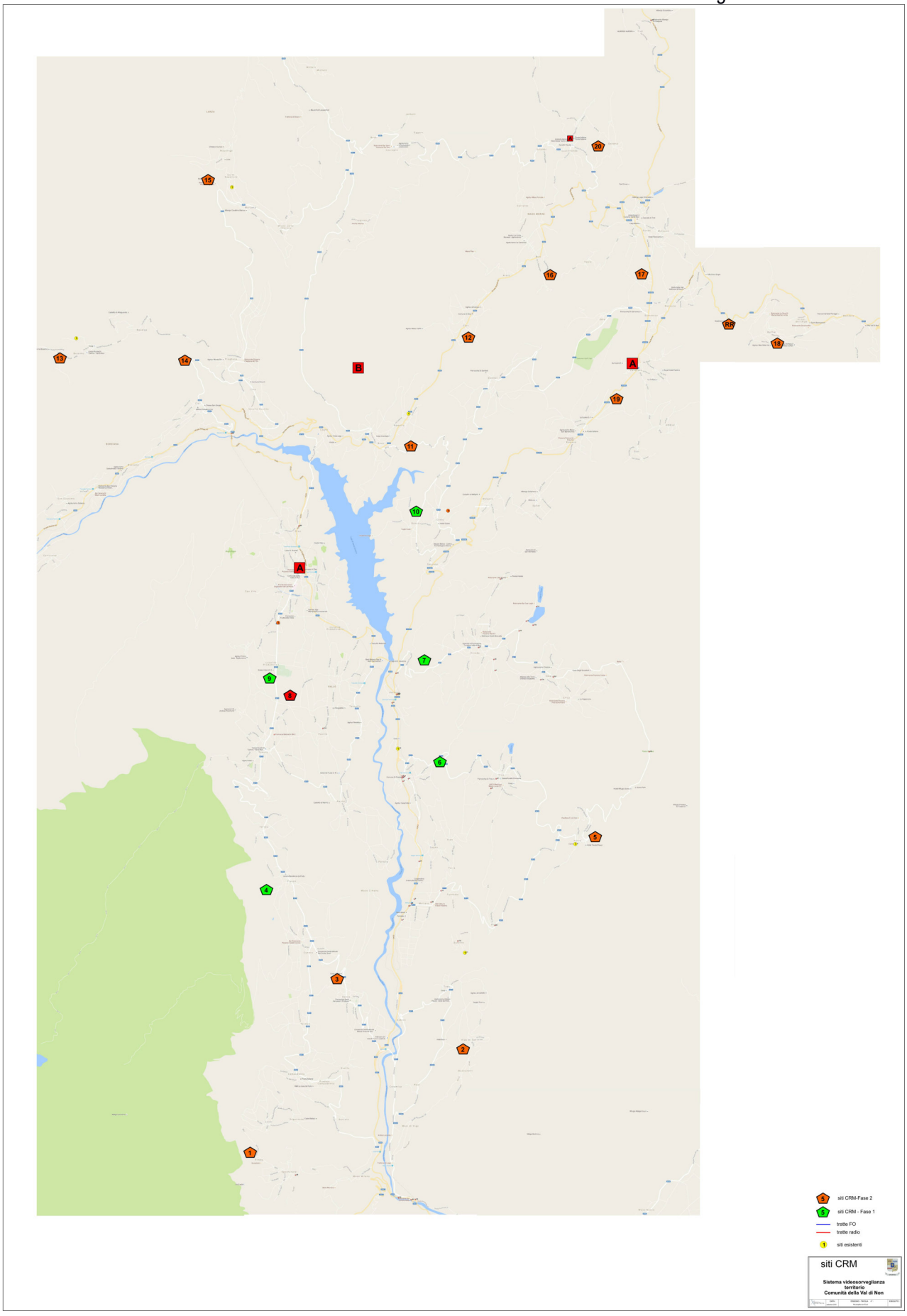
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

TRATTAMENTO IMMAGINI VIDEOSORVEGLIANZA
(art. 35 Regolamento europeo 679/2016)

1. Descrizione sistematica del trattamento

- *Il trattamento dei dati in oggetto riguarda le attività di acquisizione delle immagini tramite sistemi di videosorveglianza presso i centri di raccolta materiali (C.R.) di Cles, Taio, Coredo, Contà e Sanzeno sul territorio della Comunità della Val di Non e gestiti dalla stessa.*
- *Si è rilevato come, ormai da tempo, nei C.R. si verifichino sempre più frequentemente episodi di furti delle frazioni riciclabili dei rifiuti (in particolare batterie, RAEE e RUP) con relativi danneggiamenti, nonché episodi di abbandono di rifiuti nelle vicinanze dei centri stessi.*
  So è accertato come alcune tipologie di rifiuti oggetto di episodi di furto risultino essere, appunto, rifiuti urbani pericolosi (RUP), per i quali risulta necessario assicurare un adeguato controllo al fine di tutelare l'ambiente.
- *Si è pertanto ritenuto opportuno al fine di contrastare i fenomeni di furto, di danneggiamento e di abbandono dei rifiuti – di installare ed attivare un sistema di videosorveglianza quale efficace strumento di deterrenza e contrasto, individuando, in via sperimentale, i centri di raccolta presenti nei Comuni di Cles, Contà, Predaia e Sanzeno, in ragione del fatto che in questi ultimi risulta già attivato, un sistema di videosorveglianza gestito attraverso il Corpo intercomunale di Polizia Locale Anaunia.*
  Si è valutato come, in un'ottica di efficienza, efficacia ed economicità, opportuno che anche il sistema di videosorveglianza da attivare presso i centri di raccolta presenti nei Comuni di Cles, Contà, Predaia e Sanzeno venga gestito attraverso il Corpo intercomunale di Polizia Locale Anaunia.
  Si è ritenuto, infatti, che i soggetti istituzionalmente più adatti per realizzare l'iniziativa in oggetto siano i suddetti Comuni in quanto direttamente presenti ed operanti, attraverso il Corpo intercomunale di Polizia Locale Anaunia, sul territorio e, come tali, conoscitori privilegiati delle problematiche relative alla sicurezza pubblica ed in particolare della sicurezza urbana.
  Si è ritenuto inoltre opportuno ricomprendere nella presente iniziativa, sempre per esclusive finalità di tutela del patrimonio e di sicurezza, un ulteriore impianto di videosorveglianza da installare all'ingresso della sede della medesima Comunità e da gestire con le stesse modalità tecniche sopra descritte.
- *La finalità del trattamento risulta essere quella della tutela del patrimonio, della sicurezza e del rispetto delle normative in materia ambientale.*
- *I dati trattati risultano essere video immagini dei centri raccolta sopraccitati, con particolare riferimento alle zone di accesso ai suddetti centri e ai container dei R.U.P (rifiuti urbani pericolosi) e dei RAEE (rifiuti di apparecchiature elettriche ed elettroniche).*
  I dati vengono acquisiti tramite telecamere fisse con faro IR a controllo delle aree interessate; le telecamere sono ad alte prestazioni, rispondenti alle prescrizioni emanate dal Commissariato del Governo per la Provincia di Trento con direttiva n.2012/1063/Area1 del 06/03/2012.
  Tali telecamere sono connesse via radio e/o via cavo o fibra ottica alla sede della Polizia Locale di Cles in cui è presente il sistema di visualizzazione/registrazione e integrato il sistema radio per l'acquisizione delle telecamere.
  Tale sistema è posto in un apposito locale presso la sede della Polizia Locale di Cles, il cui accesso è strettamente controllato dalla stessa e solo il Responsabile del trattamento (comandante del corpo di Polizia Locale) o suoi incaricati possono accedere; eventuali altre persone possono farlo solo in presenza degli stessi.

- *Indicati in verde i C.R. della Val di Non interessati dal sistema di videosorveglianza*



2. Valutazione della necessità e proporzionalità del trattamento

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

3. Valutazione dei rischi per i diritti e le libertà degli interessati

Il rischio viene valutato come il prodotto della probabilità di una vulnerabilità (ovvero di una violazione di una delle proprietà della sicurezza: riservatezza – integrità – disponibilità) moltiplicato per l'impatto determinato dallo sfruttamento della stessa vulnerabilità (rispetto al diritto alla protezione dei dati personali).
Esprimendo il concetto in formula il rischio viene così espresso

*Rischio = ProbViolazione * ImpViolazione*

Le informazioni necessarie per valutare il rischio del trattamento derivano da diverse fonti come l'esperienza, la documentazione di incidenti già avvenuti, consulenze e pareri.

Per standardizzare la quantificazione delle tre probabilità di violazione delle proprietà di sicurezza e i relativi tre impatti sui diritti dell'interessato è stata definita una griglia di domande strumentali al processo di valutazione.

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

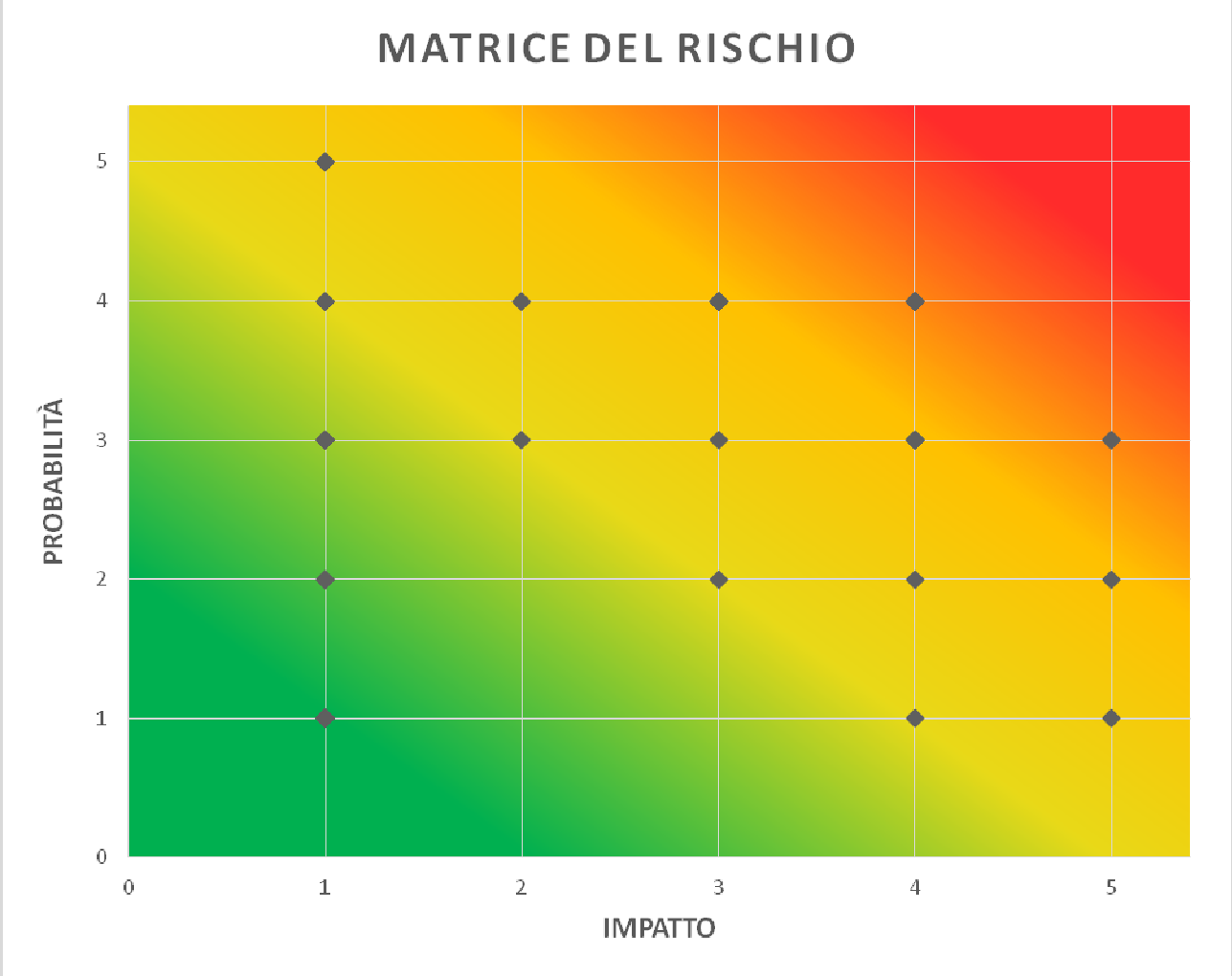
Probabilità che si verifichi una violazione di riservatezza, integrità, disponibilità

1 *evento raro (probabilità bassa)*
2 *evento improbabile (probabilità moderata)*
3 *evento possibile (probabilità elevata)*
4 *evento probabile (probabilità più che elevata)*
5 *evento quasi certo (probabilità elevatissima)*

Impatto della violazione di riservatezza, integrità, disponibilità

1 *impatto insignificante*
2 *impatto modesto*
3 *impatto moderato*
4 *impatto importante*
5 *impatto elevato*

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



Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di

controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

*Lo scorso 13 dicembre il Gruppo di Lavoro Articolo 29 (*working party *che riunisce rappresentanti dei Garanti europei) ha pubblicato delle interessanti Linee Guida relative al Data Protection Officer (aka Privacy Officer), figura chiave del nuovo regolamento europeo per la protezione dei dati personali (Regolamento UE 2016/679).*

Le linee-guida del WP29 offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Nello specifico le succitate linee- guida hanno stabilito l'obbligatorietà della valutazione di impatto in tutti i casi in cui un trattamento può presentare un livello elevato di rischio generale per i diritti e le libertà degli interessati, ai sensi dell'art. 35 del Regolamento europeo 679/2016.

Tra questi casi rientra anche il monitoraggio sistematico come ad esempio la videosorveglianza;

4. Misure previste per affrontare i rischi

Verifica delle misure di sicurezza relative alla <u>riservatezza</u> dei dati		**Si**	**No**	**Da adottare**
1	*È prevista l'autenticazione dell'utente*: tutti gli utenti, per accedere ai dati personali, devono superare un processo di autenticazione individuale	x		
2	*È prevista l'autorizzazione dell'utente*: il trattamento permette di stabilire diversi profili per singoli utenti o gruppi di essi	x		
3	*È prevista la sospensione automatica delle sessioni di lavoro*: l'applicativo disconnette automaticamente l'utente se questi non effettua operazioni per un determinato periodo di tempo		x	
4	*Gli accessi vengono registrati*: tutti gli accessi all'applicativo sono registrati in un file di log	x		
5	*I dati transitano sempre in modalità cifrata*: la comunicazione tra la postazione di lavoro ed il server avviene con protocolli sicuri (es. https)	x		
6	*L'utente deve modificare la password al primo accesso*: l'utente deve obbligatoriamente modificare la propria password al primo accesso all'applicativo	x		
7	*L'applicazione prevede profili differenziati*: l'applicativo prevede diversi profili di utente	x		
8	*L'utente può modificare la sua password*: l'applicativo permette la modifica autonoma della password	x		

9	*Le password sono criptate*: le password vengono conservate in modalità cifrata		x	
10	*La password viene modificata almeno ogni 6 mesi*: l'applicativo obbliga l'utente a modificare la password almeno ogni 6 mesi	x		
11	*È previsto il blocco dell'utente dopo un certo numero di tentativi falliti*: l'applicativo prevede il blocco dell'utente, permanente o temporaneo, dopo un certo numero di tentativi falliti	x		
12	*Esiste una procedura per il reset della password*: esiste una formale procedura per il reset delle password dimenticate	x		
13	*I dati sono trattati in un edificio/data center controllato*: i sistemi informativi utilizzati per trattare i dati sono collocati in un edificio presidiato	x		
14	*L'uso di strumenti personali per accedere a sistemi o reti istituzionali deve essere autorizzato*: i dispositivi informatici (es. portatili, cellulari, tablet) personali devono essere espressamente autorizzati per poter connettersi con la rete aziendale	x		
15	*La rete è protetta da firewall e la configurazione è mantenuta aggiornata*: la rete aziendale è protetta da un sistema di firewall con software e regole costantemente aggiornati	x		
16	*Gli accessi ad internet sono autorizzati e opportunamente filtrati: gli accessi ad internet del personale interno sono autorizzati e la navigazione è soggetta a regole per inibire il traffico verso siti non autorizzati*	x		
17	*I supporti hardware non più utilizzati vengono distrutti o resi illeggibili: esiste una procedura che prevede la cancellazione sicura, ovvero la distruzione, dei dati memorizzati su supporti non più utilizzati*	x		
18	*È vietato l'uso di supporti rimuovibili non autorizzati*: all'interno dell'azienda è vietato l'uso di supporti rimuovibili (es. usb pen) non autorizzati	x		
19	*L'accesso di fornitori di servizi alle postazioni di lavoro è regolamentato*: qualora ci si rivolga a soggetti esterni per delle attività sulle postazioni di lavoro aziendali il loro accesso è regolamentato	x		
20	*Esiste una politica che vieta la comunicazione trasmissione diffusione non autorizzate di dati personali e sensibili: tutti gli incaricati hanno ricevuto chiare istruzioni sul divieto di comunicare e/o diffondere dati personali*	x		
21	*È vietato l'uso di hardware e software non autorizzati: gli utenti possono utilizzare solo le dotazioni hardware e software espressamente autorizzate*	x		

Verifica delle misure di sicurezza relative alla <u>integrità</u> dei dati		**Si**	**No**	**Da adottare**
1	*È previsto il blocco dell'utente dopo un certo numero di tentativi falliti: l'applicativo prevede il blocco dell'utente, permanente o temporaneo, dopo un certo numero di tentativi falliti*		x	
2	*I dati sono trattati in un edificio/data center controllato: i sistemi informativi utilizzati per trattare i dati sono collocati in un edificio presidiato*	x		

3	*Tutti gli accessi all'edificio/data center sono registrati*: gli accessi ai locali dove sono conservati i dati vengono puntualmente registrati		x	
4	*I dati sono custoditi in classificatori o armadi non accessibili*: gli armadi dove sono custoditi i dati sono ad accesso controllato	x		
5	*È prevista l'autenticazione dell'utente*: tutti gli utenti, per accedere ai dati personali, devono superare un processo di autenticazione individuale	x		
6	*È prevista l'autorizzazione dell'utente*: il trattamento permette di stabilire diversi profili per singoli utenti o gruppi di essi	x		
7	*È prevista la sospensione automatica delle sessioni di lavoro*: l'applicativo disconnette automaticamente l'utente se questi non effettua operazioni per un determinato periodo di tempo		x	
8	*L'utente deve modificare la password al primo accesso*: l'utente deve obbligatoriamente modificare la propria password al primo accesso all'applicativo	x		
9	*L'applicazione prevede profili differenziati*: l'applicativo prevede diversi profili di utente	x		
10	*L'utente può modificare la sua password*: l'applicativo permette la modifica autonoma della password	x		
11	*La rete è protetta da firewall la configurazione è mantenuta aggiornata*: la rete aziendale è protetta da un sistema di firewall con software e regole costantemente aggiornati	x		
12	*Gli accessi ad internet sono autorizzati e opportunamente filtrati*: gli accessi ad internet del personale interno sono autorizzati e la navigazione è soggetta a regole per inibire il traffico verso siti non autorizzati	x		
13	*È vietato l'uso di supporti rimuovibili non autorizzati*: all'interno dell'azienda è vietato l'uso di supporti rimuovibili (es. usb pen) non autorizzati	x		
14	*L'accesso di fornitori di servizi alle postazioni di lavoro è regolamentato*: qualora ci si rivolga a soggetti esterni per delle attività sulle postazioni di lavoro aziendali il loro accesso è regolamentato	x		
15	*Esiste una politica che vieta la comunicazione trasmissione diffusione non autorizzate di dati personali e sensibili*: tutti gli incaricati hanno ricevuto chiare istruzioni sul divieto di comunicare e/o diffondere dati personali	x		
16	*È vietato l'uso di hardware e software non autorizzati*: gli utenti possono utilizzare solo le dotazioni hardware e software espressamente autorizzate	x		
17	*Il software può essere installato e configurato solo dall'amministratore*: il singolo utente non può installare software sui sistemi che trattano dati personali a meno che non sia un Amministratore del sistema		x	
18	*Viene effettuata la verifica dei dati salvati*: il processo di backup prevede verifiche, anche a campione, della leggibilità dei dati salvati		x	

Verifica delle misure di sicurezza relative alla <u>disponibilità</u> dei dati	**Si**	**No**	**Da adottare**

1	*I locali dove sono conservati i dati sono dotati di dispositivi antincendio*: i dati sono protetti dal rischio di incendio		x	
2	*I locali dove sono conservati i dati sono dotati di continuità dell'alimentazione elettrica*: i sistemi informativi dove sono conservati i dati dispongono di sistemi di alimentazione di emergenza	x		
3	*I locali dove sono conservati i dati sono dotati di controllo sull'operato degli addetti alla manutenzione*: gli addetti alla manutenzione sono supervisionati quando accedono ai locali dove si trovano i sistemi informativi che trattano i dati	x		
4	*I dati vengono salvati quotidianamente*: esiste una procedura che prevede il salvataggio almeno quotidiano dei dati	x		
5	*I backup vengono conservati anche in una location alternativa*: una copia dei dati salvati viene conservata in una location alternativa a quella principale		x	
6	*In caso di necessità i dati possono essere ripristinati entro 4 ore*: in caso di necessità è possibile ripristinare i dati eventualmente danneggiati entro 4 ore lavorative		x	
7	*I dati sono trattati in un edificio/data center controllato*: i sistemi informativi utilizzati per trattare i dati sono collocati in un edificio presidiato	x		
8	*L'utente deve modificare la password al primo accesso*: l'utente deve obbligatoriamente modificare la propria password al primo accesso all'applicativo	x		
9	*L'utente può modificare la sua password*: l'applicativo permette la modifica autonoma della password	x		
10	*La password viene modificata almeno ogni 6 mesi*: l'applicativo obbliga l'utente a modificare la password almeno ogni 6 mesi	x		
11	*Tutti gli accessi all'edificio/data center sono registrati*: gli accessi ai locali dove sono conservati i dati vengono puntualmente registrati		x	
12	*Il software può essere installato e configurato solo dall'amministratore*: il singolo utente non può installare software sui sistemi che trattano dati personali a meno che non sia un Amministratore del sistema	x		
13	*È vietato l'uso di supporti rimuovibili non autorizzati*: all'interno dell'azienda è vietato l'uso di supporti rimuovibili (es. usb pen) non autorizzati	x		
14	*L'uso di strumenti personali per accedere a sistemi o reti istituzionali deve essere autorizzato*: i dispositivi informatici (es. portatili, cellulari, tablet) personali devono essere espressamente autorizzati per poter connettersi con la rete aziendale	x		
15	*La rete è protetta da firewall la configurazione è mantenuta aggiornata*: la rete aziendale è protetta da un sistema di firewall con software e regole costantemente aggiornati	x		
16	*Gli accessi ad internet sono autorizzati e opportunamente filtrati*: gli accessi ad internet del personale interno sono autorizzati e la navigazione è soggetta a regole per inibire il traffico verso siti non autorizzati	x		
17	*I dati sono custoditi in classificatori o armadi non accessibili*: gli armadi dove sono custoditi i dati sono ad accesso controllato	x		

5. Programma di adozione di ulteriori misure di sicurezza

I dati vengono cancellati in modo irreversibile dopo 5 giorni dalla loro acquisizione.

6. Consultazione del Responsabile della Protezione dei Dati

Il titolare si è consultato ed ha inviato il presente documento di valutazione dei rischi al proprio RPD, al fine dell'acquisizione del relativo parere .

7. Ricompilare l'analisi dei rischi

In base alle misure previste da attuare è' stata compilata la Tabella (allegato 1) degli eventi e delle relative violazioni di riservatezza, disponibilità e integrità che possono accadere in relazione al trattamento dell' attività di acquisizione delle immagini tramite sistemi di videosorveglianza presso i centri di raccolta materiali (C.R.) di Cles, Taio, Coredo, Contà e Sanzeno.

La relativa matrice del rischio evidenzia l'eliminazione della classe di rischio elevata.

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

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

Cles, 15.05.2019

Firmato digitalmente
dal Presidente / Titolare del trattamento
Ing. Silvano Dominici

Consorzio dei Comuni Trentini

SERVIZIO PRIVACY - RESPONSABILE PROTEZIONE DEI DATI

Buongiorno,

con riferimento ai compiti e alle funzioni che il Consorzio dei Comuni Trentini si è impegnato a svolgere nell'ambito dell'erogazione del servizio in oggetto e, segnatamente, per quanto concerne il "Supporto nell'attività di valutazione di impatto sulla protezione dei dati" di cui al *servizio costante e continuo di supporto e consulenza quale Responsabile della Protezione dei Dati*, in merito alla Vostra richiesta pervenuta con prot. n. 4282.9 dd. 18 aprile 2019, con la presente si formula il seguente parere

Il sottoscritto Gianni Festi, nella sua qualità di Responsabile della Protezione dei Dati

premesso che

Il Titolare del trattamento, ai sensi dell'art. 5, par. 2, del Regolamento 2016/679 è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali ed in grado di comprovarlo secondo il principio della "responsabilizzazione".

Il Titolare del Trattamento, ai sensi dell'articolo 35, par. 2, del Regolamento 2016/679, ha inoltrato richiesta di consultazione relativa al trattamento di videosorveglianza.

Il Titolare del trattamento ha ritenuto che il trattamento sopra descritto presenta un rischio elevato perché incluso nell'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – Garante per la protezione dei dati personali n.467 dell'11 ottobre 2018.

Il presente parere è formulato sulla base dei seguenti atti e documenti: Schema di DPIA e relativo allegato Analisi dei rischi.

rilevato che

La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento è adeguata.

La valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità è adeguata.

La valutazione dei rischi per i diritti e le libertà degli interessati è adeguata.

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 adeguatezza al regolamento 2016/679, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone sono adeguate.

esprime parere

Favorevole

Per ulteriori informazioni si prega di contattare la dott.ssa Federica Dallaporta all'Ufficio Segreteria dell'Area Innovazione (tel. 0461 1920717 – email: servizioRPD@comunitrentini.it).

Distinti saluti.

Il Responsabile per la Protezione dei Dati
dott. Gianni Festi

Via Torre Verde, 23 – 38122 Trento – Tel. 0461 987139
info@comunitrentini.it – consorzio@pec.comunitrentini.it – www.comunitrentini.it
P.IVA e C.F. 01533550222 – iscritta al Registro delle Imprese 143476