COMUNE DI CANTELLO

# Regolamento comunale per l'attuazione del Regolamento UE 2016/679 e del D. Lgs. 101/2018 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali

**Approvato con**
**deliberazione della Giunta Comunale n. 92 del 6 novembre 2018**

## SOMMARIO

Art. 1 - Oggetto
Art. 2 - Titolare del trattamento
Art. 3 - Finalità del trattamento
Art. 4 - Responsabili del trattamento – Designati - Autorizzati
Art. 5 - Responsabile della Protezione Dati
Art. 6 - Sicurezza del trattamento
Art. 7 - Utilizzo del Sistema Informativo Comunale
Art. 8 - Registro Unico dei Trattamenti
Art. 9 - Valutazioni d’impatto sulla protezione dei dati
Art. 10 - Violazione dei dati personali
Art. 11 - Rinvio

## ALLEGATI

– Glossario Regolamento
– Glossario Registri
– Schema di registro delle attività
– Schema di Registro Unico dei Trattamenti

## Art. 1
## Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla circolazione di tali dati, nel e dal Comune di Cantello, tenuto conto del D. Lgs. 101/2018 di adeguamento del codice della privacy italiano D. Lgs. 196/2003.
2. Nell'allegato "registro delle attività" sono esplicitate tutte le azioni svolte o programmate per l'attuazione del presente regolamento, al fine di rendere conto del percorso svolto e delle misure adottate al fine di prevenire i rischi legati al trattamento dei dati delle persone.

## Art.2
## Titolare del trattamento

1. Il Comune di Cantello, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati, nonchè per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli dal n. 15 al n. 22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), del Bilancio e del Piano Risorse e Obiettivi, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
5. Il Titolare adotta misure appropriate per fornire all'interessato:
a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
6. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
7. il Titolare nomina il Responsabile della Protezione dei Dati di cui al successivo art. 5.
8. Il Titolare, inoltre, provvede a designare i Responsabili del trattamento, ovvero soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle funzioni istituzionali.
9. Inoltre, il Titolare provvede a incaricare il Designato al trattamento ovvero il dipendente della struttura organizzativa del Comune che, in costante interazione con il RPD, funge da punto di raccordo tra costui e gli Autorizzati di cui al punto successivo e informa questi ultimi circa gli adempimenti derivanti dalla normativa sulla base delle indicazioni ricevute dal RPD.

10. Infine, il Titolare e/o i Responsabili del trattamento possono prevedere, con proprio atto formale e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche appositamente Autorizzate, soggette alla loro autorità.
11. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare decisioni unitarie.
12. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

## Art.3
## Finalità del trattamento

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti compiuti per:
      - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
      - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale affidate al Comune in base alla vigente legislazione;
      → la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   b) l'adempimento di un obbligo legale al quale è soggetto il Comune;
      → la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
   c) l'esecuzione di un contratto con soggetti interessati;
   d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

## Art.4
## Responsabili del trattamento – Designati - Autorizzati

1. Il Titolare si avvale, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati in qualità di Responsabili del trattamento, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabili del trattamento e le modalità di trattamento.
2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabili del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali - tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
3. Il Titolare deve attribuire a una persona che opera sotto la sua autorità (il Designato) il compito di interfacciarsi costantemente con il RPD e gli Autorizzati e di fornire istruzioni provenienti dal RPD a questi.
4. Il Titolare e/o i Responsabili del trattamento possono attribuire specifiche attività di trattamento a persone che operano sotto la loro autorità diretta ("Autorizzati"), impartendo loro istruzioni scritte che tra l'altro individuano specificamente l'ambito del trattamento consentito. Titolare e Responsabili devono individuare le modalità più opportune per autorizzare al trattamento dei dati tali persone.

5. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato degli autorizzati anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato degli autorizzati.
6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza e/o abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, ed in particolare:
- alla tenuta del "Registro Unico dei Trattamenti" svolti per conto del Titolare, di cui al successivo art. 8;
- all'adozione di misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

## Art.5
## Responsabile della Protezione Dati

1. Il Responsabile della Protezione dei Dati (in seguito indicato con "RPD") è attualmente individuato in HALLEY LOMBARDIA SRL, ditta scelta tramite estensione di convenzione di livello sovracomunale in essere; i professionisti di riferimento risultano in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, e sono dotati di approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili e pertanto possono essere efficaci promotori di una cultura della protezione dati all'interno dell'organizzazione comunale anche nell'ambito della formazione.
2. I compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare.
Il RPD è incaricato dei seguenti compiti:
a) informare e fornire consulenza al Titolare, ai Responsabili del trattamento e al Designato in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati; in tal senso il RPD effettua per tutte le Aree funzionali un *audit* e le attività di formazione interna in tema di protezione dei dati personali; l'*audit* deve indicare a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato; la formazione dovrà essere erogata anche agli "autorizzati al trattamento" per l'ambito di competenza;
b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e dei Responsabili del trattamento; fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare, dei Responsabili del trattamento e del Designato;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare, dai Responsabili del trattamento e dal Designato;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento; il Titolare, in particolare, si consulta con il RPD in merito a:
- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione; a tali fini il nominativo del RPD è comunicato dal Titolare al Garante;
f) altri compiti e funzioni a condizione che il Titolare o i Responsabili del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi; l'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
3. Il Titolare, i Responsabili del trattamento ed il Designato assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante; nel caso in cui la decisione assunta dal Titolare o dal Responsabile interessato determini condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
4. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo; in tal senso il RPD:
a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
b) definisce un ordine di priorità nell'attività da svolgere incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed ai Responsabili del trattamento.
5. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
6. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- i Responsabili del trattamento.
7. Il Titolare, i Responsabili del trattamento e il Designato forniscono al RPD gli strumenti necessari per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti; in particolare è assicurato al RPD:
- tempo sufficiente per l'espletamento dei compiti;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note;
- accesso garantito alle aree funzionali dell'Ente così da fornire supporto, informazioni e *input* essenziali.
8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.
Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare.
Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo formalmente al Titolare ed al Responsabile del trattamento interessato.

## Art.6
## Sicurezza del trattamento

1. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione di adeguate misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

2. L’efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale, by design) sia al momento di individuare soluzioni “per impostazione predefinita” (by default), per ogni singolo trattamento.
3. Il Comune di Cantello mette in atto misure tecniche ed organizzative consone a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
4. I rischi derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
5. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
6. Costituiscono misure tecniche ed organizzative che possono essere adottate dall’Ente:
- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico.
7. Il Comune di Cantello e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
8. I dati di contatto del Titolare e del Responsabile della Protezione Dati sono pubblicati sul sito istituzionale del Comune, nella sezione “privacy” già presente.

## Art.7
## Utilizzo del Sistema Informativo Comunale

1. I riferimenti normativi oltre al GDPR sono i seguenti:
- Provvedimento a carattere generale del Garante del 27 novembre 2008 dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008;
- "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)

2. <u>Norme generali</u>

Agli utenti del Sistema Informativo Comunale non è consentito alcun accesso anonimo o non autorizzato.
Ogni utente è tenuto ad osservare le seguenti Norme Tecniche al fine di preservare la funzionalità e la sicurezza del sistema stesso e delle informazioni gestite e conservate.
Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Amministrazione.

3. <u>Norme tecniche</u>

*<u>3a. Postazioni di lavoro</u>*

Ogni postazione di lavoro viene installata con una configurazione adatta alle specifiche esigenze delle varie realtà lavorative, concordata dal Responsabile del servizio con l’Amministratore di Sistema.

La postazione si compone di:

- dotazione hardware e software
- impostazioni utente (salvaschermo, memorizzazione password, ecc.)
- autorizzazione per l'accesso a cartelle condivise e software applicativi.

Qualsiasi variazione alla configurazione della postazione di lavoro (ad esempio l'installazione di nuovi software o la rimozione o aggiornamento di quelli presenti, l'utilizzo di USB drive o altri supporti informatici, la modifica delle impostazioni utente, ecc.) deve essere preventivamente autorizzata dal Responsabile di servizio e concordata con l'Amministratore di Sistema.
Non è consentito il collegamento al Sistema Informativo Comunale di apparecchiature non di proprietà dell'Amministrazione, salvo specifica autorizzazione dell'Amministratore di Sistema.

*3B. Credenziali utente*

Ciascun utente del Sistema Informativo Comunale si connette alla rete, alle piattaforme software e alla posta elettronica, tramite autenticazione univoca personale. L'utente è tenuto a custodire e garantire la segretezza della parola chiave e a sostituirla almeno ogni sei mesi.
Le password sono modificabili da tutti gli utenti in qualsiasi momento tramite apposita procedura, specifica di ogni contesto applicativo.
I requisiti minimi di complessità delle password sono:

- redazione con caratteri maiuscoli e minuscoli
- composizione con inclusione di lettere, numeri e simboli o segni di punteggiatura
- numero caratteri non inferiori ad 8
- password non agevolmente riconducibile all'identità del soggetto che la gestisce.

Il Titolare del Trattamento dati personali può richiedere all'Amministratore di Sistema la disponibilità di dati o strumenti elettronici assegnati ad un utente in caso di sua prolungata assenza o di impedimento; ciò avviene attraverso la sostituzione della password effettuata dal AdS che la comunica al Titolare. L'AdS comunica tempestivamente e per iscritto all'utente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

*3c. Gestione dei dati*

La rete interna, istituita appositamente per permettere collegamenti funzionali tra gli utenti, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
Le cartelle di rete sono sottoposte a procedure di backup e controllo degli accessi e sono l'unico supporto sicuro sul quale memorizzare i documenti elettronici. L'utilizzo da parte degli utenti di qualsiasi altro supporto di memorizzazione (ad esempio le cartelle locali del personal computer) non garantisce la sicurezza del dato in caso di guasti hardware, sovrascritture o cancellazioni accidentali, attacchi informatici di virus o altri software malevoli.
Tutti i file di provenienza incerta o comunque esterna (Internet, posta elettronica, supporti rimuovibili), ancorché attinenti l'attività lavorativa, devono essere sottoposti al controllo antivirus.
E' vietata la cifratura di documenti effettuata autonomamente dall'utente se non concordata e autorizzata dall'Amministratore di Sistema.

*3d. Utilizzo rete Internet*

L'accesso a Internet è possibile da qualsiasi postazione connessa alla rete e costituisce parte integrante della dotazione informatica di ogni utente.
Non è consentito l'accesso a siti, social network o qualsiasi altro tipo di risorsa on-line, per scopi non inerenti la propria attività lavorativa, salvo autorizzazione concordata con l'Amministrazione Comunale.
L'Amministrazione Comunale può avvalersi di sistemi in grado di documentare il traffico internet generato dalle postazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet e il loro accesso è consentito unicamente al Titolare del trattamento dati personali e si effettuerà unicamente nei modi previsti dalla legge ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

*3e. Utilizzo posta elettronica*

Tutte le caselle appartenenti al dominio istituzionale sono di esclusiva proprietà dell'Amministrazione Comunale e il loro utilizzo è autorizzato solo per esigenze di servizio.
Lo strumento della posta elettronica non sostituisce altri sistemi più idonei per l'interscambio di documenti.

In caso di assenza programmata o prolungata, ogni utente dispone di apposite funzioni automatiche di sistema che consentono di inviare messaggi di risposta o inoltrare la posta verso differenti indirizzi.

*3f. Portale Internet comunale*

Gli utenti autorizzati possono pubblicare pagine informative e modulistica sul portale Internet comunale, utilizzando gli strumenti di redazione messi a disposizione dal Sistema Informativo Comunale.
Ogni utente è responsabile dei contenuti da esso pubblicati ed è tenuto a verificarli prima dell'effettiva pubblicazione, al fine di garantire la tutela dell'Ente.

*3g. Protezione antivirus*

Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al Sistema Informativo Comunale da parte di virus o di ogni altro software malevolo che operi con lo scopo di superare le difese di sicurezza del sistema stesso.
A tal fine, ogni utente è tenuto a:

- evitare tassativamente l'apertura di file allegati ad e-mail provenienti da utenti sconosciuti o contenenti messaggi sospetti
- segnalare tempestivamente all'Amministratore di Sistema eventuali avvisi di rischio ricevuti dal software antivirus installato o altre anomalie di funzionamento del sistema;
- evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile;
- evitare l'utilizzo di dispositivi rimuovibili (USB drive, CD/DVD, floppy disk o simili) personali o non autorizzati dall'Amministratore di Sistema;
- controllare, mediante il software antivirus, il contenuto di supporti rimuovibili autorizzati prima di ogni utilizzo.

*3h. Accesso ad archivi contenenti dati personali*

Il Comune di Cantello, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di Privacy.
L'accesso agli archivi contenenti dati personali (comuni e/o particolari) è consentito esclusivamente agli utenti autorizzati, identificati tramiti le proprie credenziali di accesso al sistema.
Ogni utente è tenuto a non allontanarsi dal proprio posto di lavoro senza aver prima chiuso la propria sessione di lavoro o bloccato in altro modo l'accesso non autorizzato al proprio sistema.

4. Responsabilità

L'utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso.
L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali di autenticazione e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'Ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.
L'utente si impegna a comunicare immediatamente all'Amministratore di Sistema l'eventuale furto, smarrimento o perdita della password. In particolare, in caso di furto, l'utente si impegna a modificare tempestivamente tale password utilizzando le procedure automatiche a sua disposizione.

## Art.8
## Registro Unico dei Trattamenti

1. Il Registro Unico dei Trattamenti reca almeno le seguenti informazioni: il nome ed i dati di contatto del Comune, del Titolare e del RPD.

   Esso si compone di due parti logiche essenziali:

   Trattamento – Dati personali – Interessati – Destinatari - Trasferimenti, recante:
   a) la sintetica descrizione e le finalità del trattamento;
   b) la sintetica descrizione delle categorie di trattamento;
   c) l'eventuale Contitolare; il Responsabile del trattamento; il Designato

d) le categorie di dati trattati (comuni cioè personali e/o particolari cioè sensibili);
e) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f) le categorie di interessati e la necessità o meno del consenso al trattamento;
g) Le categorie dei destinatari a cui i dati personali sono stati o saranno comunicati e l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

Sicurezza, recante:
h) le misure di sicurezza tecniche ed organizzative adottate in relazione al trattamento, come da precedente art. 6;
i) eventuali "autorizzati al trattamento"

2. Il Registro è tenuto dai Responsabili del trattamento, in forma telematica, secondo lo schema allegato al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni.

## Art. 9
## Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento; la DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche; fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti 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;
b) trattamenti finalizzati ad assumere decisioni automatizzate che producono significativi effetti giuridici o di analoga natura sulle persone fisiche (es. profilazione);
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o di dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
e) trattamenti di dati su larga scala, tenendo conto: della quantità di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; del volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

4. In via generale, nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati, occorre condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.
5. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa; il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.
6. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della eventuale DPIA. Il RPD monitora lo svolgimento della DPIA, se si decide di effettuarla; in tal caso, il Responsabile del trattamento interessato deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria ed il responsabile della sicurezza dei sistemi informativi deve fornire supporto al Titolare.
7. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
Il responsabile della sicurezza dei sistemi informativi può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
8. La DPIA non è necessaria nei casi seguenti:
– se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
– se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA; in questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
– se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
– se un trattamento trova la propria base legale nella vigente legislazione che lo disciplina ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
9. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati; sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i Responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- della eventuale consultazione preventiva del Garante Privacy;
c) valutazione dei rischi per i diritti e le libertà degli interessati, pesando la particolare probabilità e gravità dei rischi rilevati; sono determinati l'origine, la natura, la particolarità specifica di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure per affrontare ed attenuare i rischi, per assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.
10. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati; la mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima Autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

## Art. 10
## Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
Il Responsabile del trattamento interessato è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatasi; i rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti in condizione di fragilità e/o disagio sociale, minori, disabili, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

## Art.11
## Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti, incluso il D. Lgs. n. 196/2003 come modificato ed integrato dal D. Lgs. n. 101/2018.