

COMUNE DI CAPITIGNANIO
PROVINCIA DI L'AQUILA

REGOLAMENTO

**PER L'ATTUAZIONE DEL REGOLAMENTO (UE)
2016/679 - PROTEZIONE DEI DATI PERSONALI
DELLE PERSONE FISICHE**



INDICE

- Art. 1 - Oggetto e definizioni del regolamento*
- Art. 2 - Finalità del trattamento*
- Art. 3 - Titolare del trattamento*
- Art. 4 - Responsabili del Trattamento*
- Art. 5 - Responsabile della protezione dei dati - RPD*
- Art. 6 - Registro delle attività di trattamento del titolare*
- Art. 7 - Registro delle attività di trattamento del responsabile*
- Art. 8 - Valutazione d'impatto sulla protezione dei dati – DPIA*
- Art. 9 - Misure di sicurezza*
- Art. 10 - Violazione dei dati personali - Data Breach*
- Art. 11 - Misure per il rispetto dei diritti degli interessati*
- Art. 12 - Rinvio*

ARTICOLO 1

(Oggetto e definizioni del regolamento)

1. Il presente regolamento dispone le misure per l'attuazione del "Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

2. Ai fini del presente regolamento si intendono:

- a) *Comune*: il Comune di Capitignano, nella qualità di titolare del trattamento dei dati personali, le cui funzioni sono svolte dal Sindaco o suo delegato;
- b) *RGPD*: il Regolamento (UE) 2016/679;
- c) *Dato personale*: qualsiasi informazione che consente l'identificazione delle persone fisiche;
- d) *Interessato*: la persona fisica oggetto del trattamento dei propri dati personali;
- e) *Trattamento*: qualsiasi operazione o insieme di operazioni che può essere applicata ai dati personali;
- f) *Limitazione di trattamento*: la marcatura dei dati personali conservati soggetti a future limitazioni di trattamento;
- g) *Archivio*: qualsiasi aggregazione di dati personali accessibili secondo criteri determinati;
- h) *Titolare del trattamento (di seguito, Titolare)*: Il sindaco o suo delegato che determina le finalità e i mezzi del trattamento dei dati personali nel Comune;
- i) *Responsabile del trattamento (di seguito Responsabile)*: il soggetto che tratta i dati personali per conto del titolare del trattamento;
- l) *Responsabile della protezione dei dati (di seguito, RPD)*: il soggetto, designato dal Titolare e dal Responsabile, incaricato di fornire consulenza e assistenza per l'esatta osservanza del RGPD;
- m) *Destinatario*: il soggetto che riceve comunicazione di dati personali;
- n) *Terzo*: il soggetto che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento;
- o) *Valutazione di impatto sulla protezione dei dati (di seguito DPIA)*: procedura di valutazione di un trattamento per valutarne la necessità e la proporzionalità, nonché i relativi rischi;
- p) *Violazione dei dati personali di seguito, DATA BREACH*: qualsiasi forma di trattamento, accidentale o illecita, che comporta la distruzione, la modifica, l'accesso o la divulgazione non autorizzata dei dati personali trattati;
- q) *Autorità di controllo*: Il Garante per la protezione dei dati personali.

ARTICOLO 2

(Finalità del trattamento)

1. I dati personali acquisiti dal Comune sono trattati secondo i principi stabiliti dal RGPD e, in particolare, per l'esecuzione di dei compiti di interesse pubblico connessi all'esercizio dei pubblici poteri di cui è investito l'ente dalla normativa vigente.

2. Il trattamento dei dati è svolto, in particolare, per:

- l'esercizio delle funzioni amministrative di competenza comunale (servizi alla persona, gestione del territorio, sviluppo economico, ecc.)
- l'esercizio delle funzioni di competenza statale (stato civile, anagrafe, servizio elettorale, leva militare);
- l'adempimento di obblighi legali ai quali è soggetto il Comune;
- ulteriori funzioni amministrative di competenza statale affidate ai comuni;
- ulteriori funzioni, diverse da quelle precedenti, per le quali è stato espresso il consenso al trattamento dei dati personali.

ARTICOLO 3

(Titolare del trattamento)

1. Il Titolare del trattamento dei dati personali, contenuti in banche dati, informatiche o cartacee, gestite dagli uffici comunali, ai sensi e per gli effetti del Codice è il Comune, rappresentato dal Sindaco pro-tempore.

2. Il Sindaco, in qualità di Titolare:

- mette in atto le misure tecniche e organizzative necessarie a garantire la conformità dei trattamenti a quanto disposto dal RGPD.

- nomina con proprio atto i responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dagli articoli 13 e 14 del RGDP;
- all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in modo conforme al RGDP.

ARTICOLO 4

(Responsabili del Trattamento)

1. Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali del Comune, designa quali Responsabili del trattamento dei dati personali i dirigenti/responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento sia effettuato in conformità al RGDP.
2. I trattamenti da parte di un Responsabile sono disciplinati da atto scritto che lo vincola al Titolare e che stabilisce la durata del trattamento, la natura e la finalità del trattamento, il tipo dei dati personali e le categorie di interessati, gli obblighi e i suoi diritti.
3. Al Responsabile sono assegnati i seguenti compiti da specificare nel contratto o altro atto giuridico di nomina:
 - trattamento dei dati personali soltanto su istruzioni documentate del Titolare;
 - garanzia che i soggetti autorizzati al trattamento dei dati personali siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
 - adozione delle misure di sicurezza dei trattamenti previste dal RGDP (articolo 32);
 - ricorso ad altro responsabile del trattamento nelle forme previste dal RGDP (articolo 28, par. 2 e 4);
 - assistenza del Titolare, con misure tecniche e organizzative adeguate, per l'attuazione delle disposizioni del RGPD in materia di diritti dell'interessato (Capo III);
 - assistenza del Titolare nel rispetto degli obblighi di sicurezza dei dati personali previsti dal RGDP (articoli 32 – 36);
 - su indicazione del Titolare, disponga la cancellazione o la restituzione dei dati personali, al termine delle operazioni di trattamento;
 - messa disposizione del Titolare di tutte le informazioni riguardanti il rispetto degli obblighi dell'incarico e per lo svolgimento delle attività di revisione da parte del medesimo.
4. Il Titolare può individuare quali Responsabili, dei soggetti esterni, purché sia in possesso delle garanzie tecniche e organizzative adeguate a garantire le prescrizioni del RGPD.
5. Nel caso in cui il Titolare affidi a soggetti esterni proprie attività comportanti un trattamento di dati personali, questi saranno nominati responsabili del trattamento, unitamente al dirigente/responsabile dell'area/settore/unità di competenza.
6. Il Titolare informa ciascun Responsabile, delle responsabilità che gli sono affidate in relazione a quanto disposto dal RGDP.
7. I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata adozione delle misure di sicurezza.

ARTICOLO 5

(Responsabile della protezione dei dati - RPD)

1. Il Titolare (*e/o il Responsabile*) designa il Responsabile della protezione dei dati – RPD.
2. Il RPD è:
 - un professionista esterno, in possesso della competenza specifica della normativa e delle prassi in materia di protezione dei dati.

3. Il RPD deve essere in possesso di:

- a) un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- b) deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- c) operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

4. Il RPD è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

5. Il Titolare mette a disposizione del RDP le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.

6. Il RDP svolge i seguenti compiti:

- a) informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
- d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva, di cui all'art. 36 del RGDP.

ARTICOLO 6

(Registro delle attività di trattamento del titolare)

1. Il Titolare tiene un registro delle attività di trattamento svolte sotto la propria responsabilità.

2. Il registro contiene le seguenti informazioni:

- a) Il nome e i dati di contatto del Comune, del Titolare e del RPD;
- b) Le finalità del trattamento;
- c) Una descrizione delle categorie di interessati e delle categorie dei dati personali;
- d) Le categorie dei trattamenti effettuati;
- e) La categorie di destinatari a cui i dati personali sono o saranno comunicati;
- f) L'indicazione delle cautele specifiche, a cui ciascun responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- g) Una descrizione generale delle misure di sicurezza tecniche e organizzative;
- h) Indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

ARTICOLO 7

(Registro delle attività di trattamento del responsabile)

1. Il Responsabile del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità.

2. Tale registro contiene le seguenti informazioni:

- a) Il nome e i dati di contatto del Responsabile del trattamento e del RPD;
- b) Le categorie dei trattamenti effettuati;
- c) La categorie di destinatari a cui i dati personali sono o saranno comunicati;
- d) L'indicazione delle cautele specifiche, a cui ciascun responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- e) Eventuale possibilità di trasferimenti di dati all'estero;
- f) Una descrizione generale delle misure di sicurezza tecniche e organizzative.

ARTICOLO 8

(Valutazione d'impatto sulla protezione dei dati – DPIA)

1. La DPIA deve essere realizzata dal Titolare prima di procedere al trattamento, quando questo,

considerata sua natura, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il RPD.

3. Il Titolare definisce prioritariamente l'elenco delle tipologie di trattamenti soggette al requisito della DPIA.

4. La valutazione del rischio viene svolta tenendo conto degli elementi che costituiscono il rischio: origine, natura, gravità, probabilità, impatto sui diritti e le libertà degli interessati e deve riguardare non solo la sicurezza ma anche gli effetti complessivi del trattamento.

5. Gli aspetti riguardanti la sicurezza sono:

- disponibilità (distruzione, indisponibilità, perdita);
- integrità (alterazione);
- riservatezza (divulgazione, accesso).

6. La valutazione degli effetti complessivi del trattamento deve tenere conto dei seguenti elementi:

- Danno per la reputazione;
- Discriminazione;
- Furto d'identità;
- Perdite finanziarie;
- Danni fisici ed economici;
- Perdita di controllo dei dati;
- Altri svantaggi economico-sociali;
- Impossibilità di esercitare diritti, servizi o opportunità.

7. Le misure per la gestione del rischio (accountability) devono riguardare le seguenti aree:

- qualità dei dati;
- cifratura;
- conservazione adeguata;
- anonimizzazione dei dati;
- minimizzazione;
- misure tecnologiche (policy di sicurezza logiche e fisiche, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni);
- misure organizzative (ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti)

8. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

ARTICOLO 9

(Misure di sicurezza)

1. Il Comune, garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

2. Il Titolare e i Responsabili del trattamento mettono in atto misure e tecniche organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- a) la pseudonimizzazione e la cifratura dei dati personali trattati;
- b) procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Il Titolare e il Responsabile del trattamento fanno sì che chiunque agisce sotto la loro autorità e ha accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare.

ARTICOLO 10

(Violazione dei dati personali – Data Breach)

1. La comunicazione dell'avvenuta violazione dei dati personali è effettuata dal Titolare, senza ingiustificato ritardo, al Garante dei dati personali.
2. La notifica deve:
 - a) Descrivere la natura della violazione dei dati personali;
 - b) Descrivere le probabili conseguenze della violazione;
 - c) Descrivere le misure adottate o di cui si propone l'adozione.
3. Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione all'interessato, senza ingiustificato ritardo. La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali.
4. Non è richiesta la comunicazione qualora ricorra una delle seguenti condizioni:
 - a) Il Titolare ha messo in atto, preventivamente, delle misure e tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto di violazione, (ad esempio la cifratura);
 - b) Il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'interessato;
 - c) La comunicazione richiederebbe sforzi sproporzionati; in tal caso si procede a una comunicazione pubblica o a una misura simile tramite la quale gli interessati sono informati con analogia efficacia.

ARTICOLO 11

(Misure per il rispetto dei diritti degli interessati)

1. Il Comune adotta idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dal RGDP.
2. Le misure comprendono, in particolare:
 - a) soluzioni volte a rispettare, in relazione a prestazioni o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
 - b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
 - c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni personali;
 - d) cautele volte ad evitare che le prestazioni avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
 - e) il rispetto della dignità dell'interessato in occasione di ogni operazione di trattamento dei dati;
 - f) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati;
 - g) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

ARTICOLO 12

(Rinvio)

1. Per quanto non espressamente previsto dal presente regolamento si applicano le disposizioni del RGDP e le altre disposizioni previste in materia di tutela della riservatezza dei dati personali.