



COMUNE DI CAVATORE

REGOLAMENTO PER L'ATTUAZIONE DEL
REGOLAMENTO UE 2016/679 RELATIVO
ALLA PROTEZIONE DELLE PERSONE
FISICHE CON RIGUARDO AL
TRATTAMENTO DEI DATI PERSONALI
(GDPR)

Approvato con deliberazione del Consiglio comunale n. 20 del 28/11/2018

C.F./P.IVA 00463560060
WEB-SITE: WWW.COMUNE.CAVATORE.AL.IT
PIAZZA GIACOMO GIANOGGIO, 2 - 15010 - CAVATORE - (AL) -
PEC: COMUNE.CAVATORE@PEC.IT

COMUNE DI CAVATORE

REGOLAMENTO PER L'ATTUAZIONE DEL REGOLAMENTO UE N. 679/2016 (GDPR) E DEL D.LGS. 30/06/2003, N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI", INTEGRATO CON LE MODIFICHE INTRODOTTE DAL D.LGS. 10/08/2018, N. 101 "DISPOSIZIONI PER L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) 2016/679..."

RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

SOMMARIO

Sommario	2
Art 1 - Oggetto	3
Art 2 – Titolare del trattamento	3
Art 3 – Finalità del trattamento.....	5
Art 4 – Responsabile del trattamento.....	6
Art 5 – Responsabile della protezione dei dati.....	8
Art 6 – Sicurezza del trattamento	12
Art 7 – Registro delle attività del trattamento.....	13
Art 8 – Valutazione di impatto privacy (DPIA)	14
Art. 9 - Modalità di comunicazione	17
Art. 10 - Diffusione di dati personali.....	18
Art. 11 - Dati relativi a concorsi e selezioni.....	18
Art. 12 - Richiesta di comunicazione e di diffusione dei dati	18
Art. 13 - Consenso.....	19
Art. 14 - Diritto all'oblio	20
Art 15 – Violazione dei dati personali.....	20
Art 16 – Rinvio	25
Art 17 – Allegati.....	26

ART 1 - OGGETTO

1. Il presente Regolamento ha per oggetto misure procedurali 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 "GDPR", Regolamento Generale Protezione Dati), e del D.Lgs. 30/06/2003, n. 196 "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal D.Lgs. 10/08/2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679" relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Cavatore.

ART 2 – TITOLARE DEL TRATTAMENTO

1. Il Comune di Cavatore, rappresentato ai fini previsti dal GDPR 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"). Il Titolare può delegare le relative funzioni a Dirigente/Responsabile P.O. in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: 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 GDPR.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, 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.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. 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.

6. Il Titolare, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Dirigenti dei Settori e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici

consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. 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 GDPR. 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 GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. Il Comune di Cavatore 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 GDPR 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 di Cavatore 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 affidate al Comune in base alla vigente legislazione.

- l'erogazione del servizio Socio Assistenziale (in convenzione con A.S.C.A. Associazione Socio Assistenziale dei Comuni dell'Acquese dell'Unione Montana Suol D'Aleramo)

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 – RESPONSABILE DEL TRATTAMENTO

1. Ciascun Dirigente di Settore è nominato Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. I dipendenti del Comune di Cavatore, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi ed i diritti del Titolare del trattamento.

3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, 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 responsabile del trattamento e le modalità di trattamento.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. 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 od abbia un adeguato obbligo legale di riservatezza.

6. 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, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee 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;

- alla designazione del Responsabile per la Protezione dei Dati (RPD o DPO), se a ciò demandato dal Titolare;
- 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 DEI DATI

1. Il responsabile della protezione dei dati è designato dal Titolare in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento UE 2016/679, che di seguito sono elencati:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile 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 e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

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 GDPR;

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 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile 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.

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- 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 determina 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.

3. 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 - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

4. 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.

5. 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;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero (in relazione alle dimensioni organizzative dell'Ente) tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

7. 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 e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare, Sindaco o suo delegato, oppure al Responsabile del trattamento. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

ART 6 – SICUREZZA DEL TRATTAMENTO

1. Il Comune di Cavatore e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate 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.

2. 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.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento, con il supporto dell'Amministratore di sistema per gli aspetti tecnologici (figura interna o esterna):

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; registrazione accessi etc.);

- 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.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o

l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune di Cavatore 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.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "Privacy" eventualmente già presente.

7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

ART 7 – REGISTRO DELLE ATTIVITÀ DEL TRATTAMENTO

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome del Titolare del trattamento e del Responsabile della Protezione dei Dati (DPO);

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di 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;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa del Comune di Cavatore, in forma telematica/cartacea ed è allegato al presente regolamento.

3. Il Titolare del trattamento può decidere di affidare al Responsabile della protezione dei dati (RPD) il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

ART 8 – VALUTAZIONE DI IMPATTO PRIVACY (DPIA)

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 RGDP, 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.

4. 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.

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 DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. 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, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. 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 disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva

95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. 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;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la

natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. 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. 9 - MODALITÀ DI COMUNICAZIONE

Fuori dei casi in cui forme e modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni (cfr. art. 174, comma 12, del Codice), il Comune deve utilizzare forme di comunicazione individualizzate con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali, in particolare se sensibili, da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento

(ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

ART. 10 - DIFFUSIONE DI DATI PERSONALI

La diffusione di dati personali riferiti ai lavoratori può avvenire quando è prevista espressamente da disposizioni di legge o di regolamento (artt. 4, comma 1, lett. m) e 19, comma 3, del Codice), anche mediante l'uso delle tecnologie telematiche (art. 3 D. Lgs 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale").

Il Comune di Cavatore valorizza l'utilizzo di reti telematiche per la messa a disposizione di atti e documenti contenenti dati personali (es. concorsi o a selezioni pubbliche) nel rispetto dei principi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice).

ART. 11 - DATI RELATIVI A CONCORSI E SELEZIONI

La diffusione, che il Comune di Cavatore può lecitamente porre in essere in base a specifiche previsioni legislative o regolamentari, ha ad oggetto solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando (elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti).

ART. 12 - RICHIESTA DI COMUNICAZIONE E DI DIFFUSIONE DEI DATI

Ogni richiesta rivolta al Comune di Cavatore da soggetti privati finalizzata ad ottenere informazioni sul trattamento, la diffusione e la comunicazione dei dati personali, anche contenuti in banche dati, deve essere formulata per iscritto e debitamente motivata. In essa debbono essere specificati gli estremi del richiedente e devono essere indicati i dati ai quali la richiesta si riferisce. La

richiesta deve altresì indicare le norme di legge o regolamento che rappresentano il presupposto giuridico per la sua formulazione.

Le richieste di comunicazione e di diffusione dei dati, provenienti da altri enti pubblici od amministrazioni, sono soddisfatte ai sensi di legge o di regolamento ovvero quando siano necessarie al perseguimento dei fini istituzionali del richiedente, che quest'ultimo avrà cura di indicare, o dell'Ente.

Non è consentita la comunicazione e diffusione di dati sensibili, salvo che nei casi specificati dalla legge.

ART. 13 - CONSENSO

Ai sensi dell'art 7 del Regolamento europeo in materia di privacy, qualora il trattamento sia basato sul consenso, il Titolare deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è espresso nel contesto di una dichiarazione scritta, anche attraverso mezzi elettronici, che riguarda anche altre materie, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Per le pubbliche amministrazioni la base normativa sostituisce il presupposto del consenso, pertanto i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali.

Il Regolamento consente agli enti pubblici il recupero delle fonti vigenti, pertanto le autorizzazioni ed i provvedimenti generali adottati dal Garante, se compatibili con il nuovo quadro giuridico mantengono validità ed efficacia.

ART. 14 - DIRITTO ALL'OBLIO

E' il diritto di ogni individuo ad essere dimenticato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca.

Al venir meno dello scopo rispetto al quale i dati sono stati raccolti, l'interessato ha diritto di ottenere dal Titolare la cancellazione dei dati personali. Il Titolare dal trattamento ha l'obbligo di cancellare i dati personali resi pubblici, con la tecnologia disponibile, chiedendo la cancellazione di qualsiasi link, copia o riproduzione dei dati medesimi. Il Garante sottolinea che gli interessati potranno ottenere la cancellazione dei propri dati personali, anche on line, da parte del titolare dal trattamento se i dati sono trattati solo sulla base del consenso, se non sono più necessari per gli scopi rispetto ai quali sono stati raccolti, se sono trattati illecitamente o se l'interessato si oppone legittimamente al loro trattamento.

ART 15 – 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 di Cavatore.

2. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione

nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare, con il supporto del Responsabile della protezione dei dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. A tal fine è reso disponibile un modello per la segnalazione, predisposto dal Garante, che si allega al presente regolamento (Modello segnalazione data breach PA). La notifica è effettuata tramite posta elettronica certificata del Titolare del trattamento con l'invio del modello per la segnalazione all'indirizzo email databreach.pa@pec.gpdp.it.

3. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento 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 e contiene almeno le seguenti informazioni:

- a) la natura della violazione dei dati
- b) i dati di contatto del Responsabile della protezione dei dati
- c) le possibili conseguenze della violazione
- d) le misure adottate o di cui si propone l'adozione per porvi rimedio

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.

5. Nel caso di violazione dei dati personali il Titolare del trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.

6. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o

venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

7. Il Titolare, con il supporto del Responsabile della protezione dei dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente il Garante e l'interessato, se del caso.

8. A seguito valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della protezione dei dati, adotta una le seguenti azioni:

a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del data-breach al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento;

b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del data-breach al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/679;

c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai p.ti a) e b).

Pertanto, il Titolare del trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare al Garante che il data-breach non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

9. Ogni Responsabile di Settore, in quanto Responsabile del trattamento dei dati, per ambito di competenza, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati:

- Titolare del trattamento
- Responsabile della protezione dei dati.

La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto interno da protocollare.

Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati:

- Responsabile della protezione dei dati
- Responsabile dei Sistemi Informatici
- Responsabile del trattamento del Settore/Servizio interessato dal data-breach.

Il Responsabile della protezione dei dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.

Il Responsabile della protezione dei dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario.

A conclusione della valutazione della violazione, il Responsabile della protezione dei dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti.

10. Il Titolare del trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità.

Il registro delle violazioni è custodito dal Responsabile della protezione dei dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/679.

11. Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del Regolamento UE 2016/679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.

Il Titolare del trattamento o il Responsabile del trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

La violazione delle disposizioni contenute nel Regolamento 2016/679 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro.

ART 16 – RINVIO

Per quanto non espressamente previsto nel presente Regolamento si fa rinvio al Regolamento UE 679/2016 e successive regolamentazioni.

Il Titolare del trattamento si riserva di modificare e integrare il presente Regolamento, ove ritenuto necessario, anche alla luce di eventuali successive

innovazioni normative o pronunciamenti dell’Autorità Garante per la protezione dei dati

ART 17 – ALLEGATI

Si allega al presente Regolamento:

Allegato A: Registro delle attività del trattamento con Nomine di responsabili esterni del trattamento

Allegato B: Informativa sulla privacy da pubblicare sul sito web

Allegato C: Il modello per la notifica della violazione dei dati al Garante

Allegato D: Il modello di registro delle violazioni