UNIONE DEI COMUNI DEL COROS Unione di Comuni costituita ai sensi dell'art.32 del D.Lgs n°267/2000 e dell'art.3 e 4 della L.R.n°12/2008 tra i Comuni di Cargeghe, Codrongianos, Florinas, Ittiri, Muros, Olmedo, Ossi, Ploaghe, Putifigari, Tissi, Uri, Usini - Sede legale: Via Marconi n°14 CAP. 07045 Ossi(SS); C.F. 92108320901 – P.I. 02308440904; Tel. 0793403000 Fax 0793403041 - E mail: protocollo@pec.unionecoros.it

REGOLAMENTO DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Allegato alla delibera dell'Assemblea n. 35 **del** 30.11.2018

I N D I C E

Allegati:

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 libera circolazione di tali dati, del Comune di Siamaggiore.

ART. 2
TITOLARE DEL TRATTAMENTO[1]

1. **L'Unione dei Comuni del Coros**, rappresentato ai fini previsti dal RGPD dal Presidente pro tempore, è il Titolare (di seguito indicato con "Titolare") del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 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 e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, 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 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, 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/Responsabili P.O. 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 **dell'Unione dei Comuni del Coros**, relativamente alle banche dati gestite da soggetti esterni **all'Unione dei Comuni del Coros** 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

all'Unione dei Comuni del Coros 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 un punto di contatto comune per gli interessati.

8. L'Unione del Coros 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 **dall'Unione dei Comuni del Coros** 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 all'Unione 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 soggetta **l'Unione dei Comuni del Coros**;
   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)]

1. I Responsabili P.O. e il Segretario in cui si articola l'organizzazione dell'Ente, sono nominati Responsabili 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 RGPD.
2. I dipendenti **dell'Unione dei Comuni del Coros**, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Presidente, 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.

   Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.
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, punto 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile 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 del sub-responsabile.
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 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, 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), se a ciò demandato dal Titolare;
   - ad assistere il Titolare e l'RDP 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 e l'RDP, 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]

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato dal Titolare nella figura unica di un dipendente di ruolo **dell'Unione dei Comuni del Coros** in possesso di adeguate competenze ovvero di un'impresa o di un professionista scelto tramite procedura ad evidenza pubblica[1]. Il RPD è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.
   b) sorvegliare sull'osservanza e sull'attuazione del Regolamento Europeo, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
   c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'art. 35 del RGDP.
   d) cooperare con il Garante per la protezione dei dati personali.
   e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni

relativamente a qualunque altra questione.

f) Eseguire i propri compiti considerando debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso.
g) Riferire al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.

2. Il RDP supporta l'amministrazione nella realizzazione degli adempimenti necessari ad adeguarsi al Regolamento Europeo nella prima fase di applicazione, in particolare:
   h) Coordina l'attività degli uffici tenuti ad aggiornare e modificare il Regolamento per la gestione della privacy, secondo le indicazioni cogenti del Garante della protezione dei dati personali.
   i) Fornisce consulenza circa la predisposizione ed aggiornamento da parte di ciascun Ente del Registro delle attività di trattamento, di cui all'art. 30 del Regolamento, per una ricognizione dettagliata dei trattamenti di dati personali svolti dall'ente e verifica che questi avvengono nel rispetto dei principi fondamentali, del principio di liceità e abbiano un fondamento giuridico.

   All'interno del registro, da predisporre in formato elettronico e/o cartaceo, saranno specificati nome e contatti di riferimento del titolare del trattamento e del RDP, i trattamenti svolti e le loro principali caratteristiche specificando per ognuno:
   - finalità del trattamento;
   - categorie di dati personali coinvolti;
   - descrizione soggetti interessati;
   - categorie di destinatari cui è prevista la comunicazione di tali dati;
   - eventuali trasferimenti di dati a paesi terzi;
   - misure di sicurezza tecniche/organizzative previste dall'art. 32 del Regolamento al fine di garantire un livello di sicurezza dei trattamenti adeguato al rischio;
   - tempi di conservazione dati;
   - ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte.

   j) Fornisce un parere sui trattamenti dei dati che potrebbero generare un elevato rischio per la libertà e i diritti della persona fisica ai fini della redazione da parte dei Titolari della Valutazione d'impatto sulla protezione dei dati (art. 35 del regolamento europeo). La valutazione è svolta dagli Enti, in particolare nei casi seguenti:

   - aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
   - il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
   - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

   La valutazione d'impatto contiene almeno:
   - una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
   - una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
   - una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
   - le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

   k) Sorveglia e fornisce consulenza ai Titolari sull'attuazione ovvero aggiornamento delle misure tecniche ed organizzative e sugli atti e documenti per garantire che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina.
   l) Fornisce supporto al Titolare, in accordo con le Figure competenti, circa le azioni necessarie per l'adeguamento alle disposizioni AGID in materia di misure idonee per la sicurezza informatica.
   m) Fornisce consulenza sulle problematiche relative alla tutela dei dati personali e alla sicurezza informatica.

n) Programma almeno due giornate all'anno di consulenza e formazione interna, dedicate ai dipendenti **dell'Unione dei Comuni del Coros**. Resta inteso che in caso di modifiche normative sostanziali si programmerà un intervento formativo ad hoc.

3. Le attività descritte al punto 2 costituiscono altresì oggetto del servizio.

4. Al fine di poter espletare al meglio il servizio, è riconosciuta al RDP la possibilità di accedere agli archivi, di assumere informazioni dagli autorizzati al trattamento, chiedere informazioni e documenti su circostanze specifiche ed eventi accaduti, segnalando eventuali inosservanza al Titolare del trattamento.

5. Nel caso di RDP esterno è, altresì, riconosciuta la facoltà di indicare il soggetto Referente che fungerà da punto di contatto tra l'amministrazione comunale e lo stesso RDP.

6. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
   b) il Responsabile del trattamento;
   c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

7. Nello svolgimento dei compiti affidatigli il RPD dovrà:
   a) svolgere i compiti che gli spettano secondo quanto previsto dal presente regolamento osservando le norme in materia di segreto, riservatezza e confidenzialità, la normativa nazionale ed europea vigente in materia;
   b) eseguire i propri compiti considerando preventivamente i rischi inerenti al trattamento;
   c) utilizzare le eventuali risorse che il Titolare e i Responsabili del trattamento gli forniscano al fine di assolvere al meglio ai compiti attribuitigli dalla legge, accedere ai dati personali e ai trattamenti nonché di rafforzare la propria conoscenza specialistica;
   d) operare in modo indipendente;
   e) riferire direttamente al Presidente **dell'Unione dei Comuni del Coros**, qualora ritenga che il Responsabile e/o il Titolare del trattamento assumano decisioni incompatibili con il RGPD;
   f) informare immediatamente il Presidente qualora sia destinatario di qualsiasi atto di intimidazione nel corso del proprio servizio che abbia l'obiettivo di condizionarne la regolare e corretta esecuzione;
   g) mettere a disposizione un recapito postale, telefonico fisso e/o mobile ed un indirizzo di posta elettronica utili alla reperibilità.

   Al RDP è riconosciuta la facoltà di:
   - costituire uno staff formato da soggetti, in possesso dei requisiti richiesti dal Regolamento europeo, che operano sotto la direzione del RDP che lo supportano ai fini del corretto svolgimento delle proprie funzioni;
   - qualora lo necessiti, accedere ad altri servizi all'interno della struttura del Titolare e/o Responsabile del trattamento così da ricevere tutto il supporto, le informazioni o gli input necessari.

8. Durante lo svolgimento del servizio, i Titolari del Trattamento dovranno:
   a) Coinvolgere tempestivamente ed adeguatamente il RDP per mezzo del Referente incaricato e dei Responsabili del trattamento in qualsiasi questione inerente la protezione dei dati personali.
   b) Mettere a disposizione del RDP le risorse necessarie all'esecuzione dei propri compiti, il Referente ed eventualmente un gruppo di lavoro, formato dai Responsabili del Trattamento, in possesso delle competenze tecniche e informatiche e della necessaria conoscenza dei procedimenti e dei processi di lavoro degli Enti.
   c) Non rimuovere o penalizzare il RDP in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.

d) Garantire che il RDP eserciti le proprie funzioni in autonomia e indipendenza e, in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto d'interesse.

ART. 6
SICUREZZA DEL TRATTAMENTO[(2)]

1. **L'Unione dei Comuni del Coros** e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per 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:
   a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   b) 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. **L"Unione dei Comuni del Coros** 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 **dell'Unione dei Comuni del Coros**, 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).

ART. 7
REGISTRO UNICO DELLE ATTIVITÀ DI TRATTAMENTO ART 30 COMMI 1 E 2 DEL GDPR

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto **dell'Unione dei Comuni del Coros**, del Presidente -, eventualmente del Contitolare del trattamento, del RPD, del soggetto delegato dal Titolare alla tenuta ed aggiornamento del Registro;
   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, presso gli uffici della struttura organizzativa **dell'Unione dei Comuni del Coros** in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
4. Il Titolare tiene un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti nonché le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personaliil Titolare delega la sua tenuta al ad un solo Responsabile del trattamento nominato Referente con separato atto, ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

ART. 8
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 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. 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) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   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 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: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; 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.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, 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.

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 **dell'Unione dei Comuni del Coros**. 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; 0 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 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 RGPD, 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.
11. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

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 **dall'Unione dei Comuni del Coros**.
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 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 verificatesi. 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 deboli, minori, 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.

Note

(1) Il Titolare del trattamento (cioè il Presidente o suo delegato, individuato tra i Dirigenti/Responsabili P.O. in possesso di adeguate competenze) dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, 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. A tali fini mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia 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 e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
Il Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza viene nominato dal Titolare del trattamento tra uno o più Dirigenti/Quadri/Responsabili di U.O. delle strutture di massima dimensione in cui si articola l'organizzazione **dell'Unione dei Comuni del Coros**. Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative di cui all'art. 5 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD. E' consentita la nomina di sub-responsabili del trattamento (gli incaricati del trattamento nel Codice Privacy) da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare dell'inadempimento, dell'operato del subresponsabile, 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 sul suo operato.
Il Responsabile della protezione dei dati ha il compito di controllare l'efficacia e della sicurezza dei sistemi di protezione dei dati personali. Può essere scelto fra i dipendenti del,Ente di qualifica non inferiore alla cat. D (oppure C negli enti di minore dimensione), purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il Responsabile della protezione dei dati mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il Responsabile della protezione dei dati non sia un dipendente dell'Ente, l'incaricato persona fisica è selezionato mediante procedura ad evidenza pubblica fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al RPD sono indicati in apposito contratto di servizi. Il Responsabile della protezione dei dati esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare ed al Responsabile del trattamento. Nel caso di Enti/Comuni di minori dimensioni demografiche, è possibile l'affidamento dell'incarico di Responsabile della protezione dei dati ad un unico soggetto, anche esterno, designato da più Enti mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto 2000 n. 267.

(2) L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che 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. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

Allegati : A) Schema di Registro unico dei trattamenti. GLOSSARIO REGOLAMENTO

Ai fini della proposta di Regolamento comunale, si intende per:

- **Titolare del trattamento:** l'autorità pubblica **dell'Unione dei Comuni del Coros** o altro ente locale che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

- **Responsabile del trattamento:** il Dirigente/Responsabile P.O., oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

- **Sub-Responsabile del trattamento:** il dipendente della struttura organizzativa **dell'Unione dei Comuni del Coros**, incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

- **Responsabile per la protezione dati – RPD:** il dipendente della struttura organizzativa **dell'Unione dei Comuni del Coros**, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.

- **Registri delle attività di trattamento:** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.

- **DPIA -Data Protection Impact Assessment**" -"**Valutazione d'impatto sulla protezione dei dati:** è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

- **Garante** Privacy: il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

- **Categorie di trattamento:** Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

- **Categorie di dati personali:** Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita Situazione economica, finanziaria, patrimoniale, fiscale. Dati di connessione: indirizzo IP, login, altro. Dati di localizzazione: ubicazione, GPS, GSM, altro.

- **Finalità del trattamento:** Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, 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 di Siamaggiore. Adempimento di un obbligo legale al quale è soggetto il comune di Siamaggiore. Esecuzione di un contratto con i soggetti interessati. Altre specifiche e diverse finalità.

- **Misure tecniche ed organizzative:** Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi. Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) -adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso. Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico -adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso. Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

- **Dati sensibili:** Dati inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali.

- **Categorie interessati:** Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

- **Categorie destinatari:** Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.