ALLEGATO A

ATTO ORGANIZZATIVO PER L'ATTUAZIONE DELLA NORMATIVA IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI.

Art.1 – Oggetto.

1. Il presente Atto disciplina gli aspetti organizzativi interni all'Ente per l'applicazione della normativa in materia di trattamento dei dati personali, in attuazione del Regolamento UE 2016/679 (di seguito "Reg.UE", della normativa nazionale e dei provvedimenti generali adottati dal Garante per la protezione dei dati personali;

2. Nell'applicazione della normativa in materia di trattamento dei dati personali devono essere perseguite soluzioni e modalità semplificate che limitino l'impatto sulla struttura amministrativa dell'Ente.

3.In applicazione di quanto disposto dall'art.25 del Reg.UE, i trattamenti di dati personali all'interno dell'Ente devono sottostare ai seguenti principi:

- sin dall'inizio di una nuova tipologia di trattamento (fase di progettazione) la scelta delle modalità e dei mezzi utilizzati deve basarsi sulla necessità del rispetto della riservatezza e dei diritti fondamentali degli interessati ("privacy by design") ;

- l'impostazione e l'organizzazione dei processi lavorativi deve costantemente sottostare a detta necessità, al fine di trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento ("privacy by default").

Art.2 – Titolare del trattamento dei dati e Designati

1. Ai sensi degli artt. 4 punto 7) e 24 del Reg.UE, titolare del trattamento dei dati da parte della struttura organizzativa del Comune di Fiumefreddo di Sicilia è lo stesso Ente, che nel rispetto ed in attuazione della vigente normativa, esercita potere decisionale sulle finalità e sui mezzi del trattamento dei dati personali, ivi compreso il profilo della sicurezza.
2. Il Sindaco
• si relaziona direttamente con il responsabile della protezione dei dati di cui all'art.8, nello svolgimento delle funzioni ivi previste ;
• attiva iniziative formative interne all'Ente allo scopo di diffondere la conoscenza e la corretta applicazione della normativa in materia di trattamento dei dati personali;
• mette in atto misure tecniche ed organizzative adeguate a garantire, ed a essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al General Data Protection Regulation n. 679/16 (R.G.P.D.);
• può attivare forme di verifica circa il rispetto, da parte degli uffici, delle norme e disposizioni in materia di trattamento dei dati personali;
• approva i modelli per i registri dei trattamenti, per le valutazioni di impatto e per altre finalità di attuazione degli istituti in materia
• procede alla designazione e nomina degli organismi monocratici e collegiali previsti dalla normativa e rimessi alla determinazione del titolare con particolare riferimento al DPO-RPD, Responsabili esterni, Designati interni, gruppi di lavoro e team di progetto a supporto delle attività specifiche;
• svolge gli ulteriori atti ed attività previste nel presente Atto Organizzativo.

3. I Responsabili di Posizione Organizzativa e il Comandante di Polizia Municipale nell'ambito delle dotazioni e risorse messe a disposizione e secondo gli indirizzi degli atti di pianificazione e programmazione comunale, adottano tutti gli atti a rilevanza esterna ivi compresi gli incarichi, affidamenti, convenzioni ed accordi per la corretta attuazione di quanto previsto dal GDPR nel rispetto della disciplina di settore con particolare riferimento alla L. 241/1990, Dlgs 82/2005, Dlgs 50/2016; i predetti Responsabili ricoprono automaticamente la funzione di organo designato dal Titolare per lo svolgimento delle relative competenze.

Art.3 – Contitolare del trattamento dei dati.

1. Nel caso di esercizio associato e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorchè due o più titolari determinano congiuntamente mediante accordo le finalità ed i mezzi del trattamento, si realizza la contitolarità del trattamento di cui all'art.26 del Reg.UE.
2. Presupposto per la contitolarità è la condivisione tra diversi titolari delle finalità e dei mezzi del trattamento dei dati personali
3. I rispettivi ruoli ed obblighi per gli aspetti concernenti il trattamento dei dati devono essere regolati all'interno di un accordo/protocollo/contratto che 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;

Art.4 – Responsabili del Trattamento dei Dati

1. Ai sensi degli artt.4 punto 8) e 28 del Reg.UE, il Responsabile del Trattamento dei Dati per conto del Comune è nominato per iscritto nell'ambito di contratti, accordi o altra tipologia di atto giuridico che definisce la nomina della persona fisica o giuridica responsabile e, con riferimento al trattamento dei dati, la finalità, la tipologia dei dati, la durata del trattamento, gli obblighi e le modalità del trattamento.

2. Il Responsabile del trattamento dei dati 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.

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, 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 da parte del 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 od 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 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.

8. Possono essere designati responsabili del trattamento i soggetti che per esperienza, capacità ed affidabilità forniscano le garanzie previste dalla predetta norma.
9. Il Responsabile del trattamento designato individua i soggetti autorizzati al trattamento.

Art.5 – Ruolo della dirigenza all'interno del Comune.

1. All'interno dell'organizzazione del Comune i Responsabili di Posizione Organizzativa e il Comandante di Polizia Municipale, assegnatari di risorse umane, strumentali e finanziarie, nonché soggetti dotati di competenze e responsabilità gestionali, presidiano all'interno dell'unità organizzativa assegnata il rispetto della normativa in materia di trattamento di dati personali.

All'interno della Polizia locale tale funzione di ausilio è esercitata da altri dipendenti con posizione di responsabilità in relazione alla specifica organizzazione del Corpo di Polizia locale.

Art.6 – Soggetti autorizzati al trattamento dei dati.

1. Tutti i dipendenti o altri soggetti che operano all'interno della struttura comunale sono autorizzati al trattamento dei dati personali nel rispetto delle indicazioni, istruzioni o limiti individuati dal Responsabile dell'unità organizzativa di assegnazione, ai sensi dell'art.4 punto 10) del Reg.UE ("persone autorizzate al trattamento").
2. Le modalità di autorizzazione sono individuate dal Responsabile in relazione all'organizzazione degli uffici ed alle tipologie dei trattamenti
3. In relazione all'organizzazione dell'unità organizzativa, alle funzioni svolte ed alla tipologia di trattamenti e di dati trattati, il Responsabile può con disposizione di servizio:
- specificare la tipologia e le modalità di trattamento ammissibili per i dipendenti assegnati
- specificare le eventuali prescrizioni particolari volte a garantire la riservatezza e la sicurezza nel trattamento dei dati
- individuare particolari limiti od esclusioni al trattamento per determinati dipendenti.

4. Tra i soggetti autorizzati al trattamento può essere individuato un "referente privacy" di Settore/Unità di staff/Unità di progetto.

Art.7 – Amministratori di sistema.

1. Le funzioni di "amministratore di sistema", nei diversi profili funzionali previsti, sono attribuite per iscritto dal Responsabile del Settore preposto alla gestione di sistemi informativi, sentito il Segretario Comunale. A tal proposito, in considerazione dell'assenza di profili professionali dotati di specifiche competenze tecniche, l'Amministrazione, compatibilmente con i vincoli di bilancio, si impegna a provvedere alla formazione del personale, affinchè l'Ente possa assicurare l'attuazione di sufficienti misure di sicurezza ICT. Il Responsabile ICT evidenzierà le attività di programmazione e gli investimenti necessari.
Fornirà periodiche indicazioni operative per la salvaguardia della sicurezza informatica (come ad es.: utilizzo di PW; divieto di utilizzo di applicativi non autorizzati, utilizzo di cartelle di rete; obbligo di accettare aggiornamenti sui dispositivi/applicativi, ecc...).

Art.8 – Responsabile della protezione dei dati. (RPD)

1. Il Responsabile della protezione dei dati, di cui agli artt.37-38-39 del Reg.UE, è nominato con provvedimento del Sindaco, tenendo presenti i requisiti indicati nelle predette norme e specificandone i compiti nell'ambito delle funzioni di consulenza, sorveglianza e contatto con il Garante.

2. La funzione di consulenza può essere svolta anche nell'ambito di iniziative formative. La funzione di sorveglianza può essere svolta anche mediante specifiche richieste ai responsabili del trattamento, sempre in un'ottica di collaborazione e di miglioramento nell'applicazione degli istituti relativi alla materia del trattamento dei dati personali.
Il responsabile della protezione dei dati mantiene uno stretto rapporto di collaborazione con il Segretario generale e con il Responsabile del Settore preposto alla gestione dei sistemi informativi.
3. Qualora la designazione verta su un soggetto esterno all'Ente, le modalità di affidamento delle relative attività sottostanno alla normativa in materia di appalti ("contratto di servizi" ai sensi dell'art.37 c.6 del reg.UE).
4. In ogni caso detta figura opera in autonomia ed indipendenza, relazionandosi direttamente con il Segretario Comunale quale vertice gestionale dell'Ente.
5. Al Responsabile della Protezione dei dati sono affidati i compiti di cui all'art.39 del Reg.UE, declinati e precisati all'interno dell'atto di designazione/affidamento, che vengono svolti in interlocuzione e confronto con i singoli dirigenti.
6. Il responsabile della protezione dei dati nominato ha l'obbligo di astenersi nel caso sussistano condizioni di conflitto di interesse.

ART. 9 GRUPPO DI LAVORO GDPR

1. E' istituito un gruppo di lavoro permanente in materia di adattamento alle norme del GDPR composto da:
- segretario comunale con compiti di impulso e coordinamento
- Responsabili di Servizi e Comandante di P.M.
- uno o più membri designati dai Responsabili di P.O. e dal Comandante di P.M. in relazione alla competenza, preparazione e/o ruolo nel trattamento di dati particolari
- almeno un referente del servizio ICT quale supporto tecnico per le problematiche di sicurezza tecnologica
- il DPO-RPD (eventuale) invitato in occasione della trattazione di particolari tematiche
2. Le riunioni del gruppo sono tracciate, verbalizzate e gli esiti, sono resi pubblici mediante apposita sezione del sito internet comunale.
3: Il gruppo di lavoro definisce ed aggiorna in particolare:
- un programma permanente di informazione e formazione del personale
- le priorità di intervento per l'adattamento al GDPR
- le misure "minime" da adottare per il rispetto della normativa
- la modulistica uniforme sia ad uso esterno che ad uso interno (informativa, consenso, comunicazioni, registri ecc...)
- la redazione e l'aggiornamento dell'elenco dei responsabili e dei designati

Art. 10 – Registri delle attività di trattamento.

1. Il registro di cui all'art.30 del Reg.Ue del titolare del trattamento, contenente le informazioni minime ivi previste, è distinto in sezioni ed è predisposto, in formato e con firma digitale, a cura dei singoli Responsabili di P.O. secondo le modalità stabilite nell'ambito di attività del Gruppo di Lavoro di cui all'art. 9; l'ambito della singola sezione fa riferimento all'unità organizzativa assegnata al Responsabile.
2. Le singole sezioni vengono tenute aggiornate, con nuova protocollazione del documento, in relazione ad eventuali modifiche delle attività di trattamento e comunque almeno una volta ogni 12 mesi.
3. Il Gruppo di lavoro cura l'aggiornamento del registro delle attività di trattamento di cui all'art. 30 del GDPR, adeguando la versione iniziale allegata al presente atto, mediante acquisizione dai Responsabili dei servizi i dati e le informazioni sulle tipologie di trattamento secondo il modello.
3. Il registro è in formato elettronico, facilmente accessibile a tutti i soggetti autorizzati alla sua redazione ed è fruibile direttamente, senza intermediazione, da parte del DPO- RPD e dell'autorità di controllo.
4. Il registro, depurato di eventuali informazioni non necessarie o che possano mettere a rischio la sicurezza dell'Ente è pubblicato sul sito internet nella sezione dedicata al GDPR.

Art.11 – Valutazione di impatto sulla protezione dei dati (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. 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.
4 La valutazione, da effettuare a livello della singola unità organizzativa, è predisposta e sottoscritta, in formato e con firma digitale, a cura del singolo Responsabile.
5. Le singole valutazioni di impatto vengono tenute aggiornate, con nuova protocollazione del documento, in relazione ad eventuali modifiche delle attività di trattamento.

Art.12 – Comunicazione di dati a soggetti terzi.

1. I dati personali possono essere comunicati a soggetti pubblici o privati oppure diffusi ove previsto da una norma di legge o di regolamento.

2. in applicazione del c.1, si prevede che la comunicazione sia ammessa anche qualora i dati comunicati siano necessari per lo svolgimento di attività da parte di soggetti terzi sulla base di un
rapporto costituito tra il Comune e gli stessi in base ad un contratto, un accordo, un protocollo di intesa o un incarico formalizzati.
Tale rapporto deve avere a fondamento le esplicitate finalità istituzionali di pubblico interesse del Comune o comunque finalità di pubblica utilità.
La comunicazione di dati può avvenire anche mediante l'accesso selettivo (con riferimento ai soggetti che accedono ed ai dati oggetto di accesso) alle banche dati del Comune.

3. All'interno dell'atto di formalizzazione del predetto rapporto devono essere specificati l'eventuale ruolo di responsabile (esterno) del trattamento per conto del Comune rivestito dal soggetto terzo e le prescrizioni dettate per garantire la sicurezza nel trattamento.
Nel medesimo atto devono inoltre essere specificate le finalità di interesse pubblico, le tipologie di dati e di trattamenti consentiti al terzo.
Tali prescrizioni sono modulate sulla base della tipologia di dati, della categoria di soggetti interessati e delle finalità del trattamento.

Art.13 - Misure di sicurezza.

1. I responsabili (esterni) del trattamento dei dati ed i Responsabili di Posizione Organizzativa e il Comandante di P.M. mettono in atto misure di sicurezza tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio ed attuano tali misure applicandole alla specificità delle categorie e tipologie di dati trattati, alle caratteristiche dei luoghi ed alla strumentazione disponibile.
L'adozione delle misure di sicurezza avviene in compatibilità con la disponibilità di spazi fisici, con gli assetti logistico - organizzativi e con la disponibilità di strumenti e tecnologie.
2. Con apposito documento, predisposto e sottoscritto in formato digitale, vengono individuate le misure di sicurezza adottate in ambito informatico all'interno dell'Ente; tale documento, per il carattere di riservatezza del medesimo, è sottratto alla pubblicazione ed all'accesso da parte di terzi soggetti.
3. Il Segretario Comunale, sentito il Responsabile per la Protezione dei Dati, può predisporre codici di condotta per il trattamento dei dati personali.

Art.14 – Violazione dei dati personali (data breach).

1. Ai sensi dell'art.4 punto 12) del Reg.UE, costituisce "violazione dei dati personali" una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
2. La procedura di notifica all'Autorità di controllo (Garante privacy) prevista dal Regolamento UE 679/2016 (artt.33-34) viene attivata, qualora sia stimato come probabile un rischio per i diritti e le libertà delle persone fisiche, con la segnalazione da parte del dirigente al Segretario comunale ed al responsabile della protezione dei dati; la segnalazione deve avvenire entro 24 ore dall'evento.
3. Nella segnalazione, da formulare per iscritto, viene fatta descrizione del tipo di violazione, delle circostanze e dei dati e delle persone fisiche interessate.
4. Il Segretario comunale, consultato preventivamente il responsabile della protezione dei dati, effettua la notifica della violazione all'Autorità di controllo (Garante della privacy) e, ove previsto, agli interessati dal trattamento (persone fisiche a cui si riferiscono i dati oggetto di violazione); il Segretario comunale dispone verifiche in merito alle cause che hanno determinato la violazione stessa.
5. Anche nel caso di mancata notifica all'Autorità di controllo per assenza di rischi per i diritti e le libertà delle persone fisiche, la violazione dei dati è oggetto di analisi e documentazione da parte dell'unità organizzativa interessata.

Art.15 – Informativa agli interessati.

1. I Responsabili di Posizione Organizzativa e il Comandante di Polizia Municipale curano, all'interno delle unità organizzative di riferimento, l'attuazione dell'informativa agli interessati prevista dagli artt.13-14 del Reg.UE.

2. Tale attuazione può avvenire tramite:
- avvisi generali sul sito dell'Ente
- avvisi generali interni agli uffici
- avvisi generali esterni agli uffici
- informativa all'interno della modulistica/dei provvedimenti/dei contratti
- comunicazioni mirate agli interessati
- altri mezzi comunicativi individuati dal dirigente per ottemperare alle finalità di cui alle predette norme.

3. La scelta dei mezzi attraverso cui rendere l'informativa viene valutata dal dirigente anche sulla base della tipologia di utenza, del numero di utenti da informare, delle caratteristiche dei trattamenti dati previsti.
In relazione agli specifici procedimenti amministrativi di interesse e considerata l'ampia articolazione e la diversificazione di tipologia degli stessi, oltre all'utilizzo dei predetti canali informativi maggiori informazioni sulle finalità, modalità e tipologie di trattamento dei dati personali vengono fornite verbalmente, a richiesta degli interessati, da parte degli uffici delle singole unità organizzative. I dirigenti si accerteranno della corretta formazione dei dipendenti addetti al rilascio di tali informazioni.
4. l'informativa viene resa in una forma ed un linguaggio concisi, trasparenti, intelligibili e facilmente accessibili.

Art.16 – Rapporti con il Garante (Autorità di controllo).

1. Per quanto concerne gli aspetti di contatto nei rapporti con il Garante per la protezione dei dati personali, gli stessi sono svolti dalla figura del Responsabile della Protezione dei Dati nell'ambito dei compiti allo stesso assegnati dall'art.39 del Reg.UE.
2. Al fine di garantire una supervisione da parte del vertice gestionale dell'Ente, le eventuali comunicazioni formali al Garante per la protezione dei dati personali sono sottoscritte anche dal Segretario Comunale.