

Comune di Mestrino

(Provincia di Padova)



Regolamento Comunale per l' attuazione del Regolamento Generale Europeo per la Protezione dei Dati UE nr. 679/2016

Deliberazione del Consiglio Comunale n. 25 del 29-7-2019

INDICE

Art. 1	Oggetto	2
Art. 2	Finalità	2
Art. 3	Definizioni	4
Art. 4	Soggetti	5
Art. 5	Responsabile del Trattamento	7
Art. 6	Responsabile comunale della protezione dei dati	8
Art. 7	Adozione “ Registro delle attività di trattamento e delle categorie delle attività	10
Art. 8	Trattamento dei dati personali	11
Art. 9	Coordinamento con Amministrazione Trasparente, procedimenti di acceso civico, generalizzato e documentale.	12
Art. 10	Formazione del Personale	12
Art. 11	Trattamenti consentiti	12
Art. 12	Principi	13
Art. 13	Attività Amministrativa	13
Art. 14	Fascicolo personale dipendenti e amministratori	14
Art. 15	Sicurezza dei dati- misure di sicurezza – verifiche e controlli	14
Art. 16	Trattamento e accesso ai dati sensibili e giudiziari	15
Art. 17	Diritti dell’ interessato	16
Art. 18	Valutazione d’ impatto sulla protezione dei dati	16
Art. 19	Violazione dei dati personali	20
Art. 20	Entrata in vigore e normativa applicabile	21
Art. 21	Rinvio dinamico	21
Art. 22	Norme abrogate	21
Art. 23	Pubblicità del Regolamento	21

Art. 1 - Oggetto del regolamento

1. Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite od utilizzate dall'amministrazione comunale, in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione:

- della normativa in materia di diritto di accesso documentale, accesso civico e accesso generalizzato
- del Regolamento UE 2016/679 del 27 aprile 2016 relativo alla "*protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" e che abroga la direttiva 95/46/CE.

Art. 2 - Finalità

1. Il comune, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza ed all'identità personale nonché delle norme vigenti in materia di protezione e gestione dei dati.

2. In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi del comune, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.

3. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità;

4. Ai fini del presente regolamento, per finalità istituzionali del comune si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.

5. I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- *l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;*

- *la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;*

- *l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale*

affidate al Comune in base alla vigente legislazione.

- 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) le specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 3 - Definizioni

1. Ai fini del presente regolamento si intende per:

- a) **"trattamento"**: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*
- b) **"dato personale"**: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*
- c) **"dati identificativi"**: *i dati personali che permettono l'identificazione diretta dell'interessato;*
- d) **"dati sensibili e giudiziari"**: *dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché la trattazione di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.* (cfr. **ALLEGATO n. 1**, contenente i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili).
- e) **"titolare del trattamento"**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono*

determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;;

- f) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*
- g) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*
- h) "interessato", la persona fisica, cui si riferiscono i dati personali;*
- i) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*
- j) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*
- k) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;*
- l) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;*
- m) "Garante", l'autorità preposta al controllo della privacy.*
- n) "violazione di dati personali": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.*
- o) "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;*
- p) "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e*

soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Art. 4 – Soggetti

1. Il Comune di Mestrino, rappresentato, in ossequio al Regolamento UE 2016/679, dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con “*Titolare*”).

2. Il Titolare è responsabile del rispetto dei principi contenuti nell’art. 5 del Regolamento UE 2016/679:

liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare adotta misure appropriate per fornire all’interessato:

a) le informazioni indicate dall’art. 13 del Regolamento UE 2016/679, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall’art. 14 del Regolamento UE 2016/679, qualora i dati personali non stati ottenuti presso lo stesso interessato.

4. 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, del Reg. citato, considerati la natura, l’oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

5. Il Titolare, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Responsabili P.O. 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 qualora sia scelto tra i dipendenti del Comune;

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. Tale attività può essere dal Titolare delegata al Responsabile del Trattamento;

*d) **nominare** un Amministratore di sistema a cui spetta il compito di supportare il Titolare e/o il Responsabile del trattamento nel mettere in atto le misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 27 aprile 2016 n.679). Tale attività viene delegata al Responsabile del Trattamento qualora l' Amministratore di Sistema venga scelto tra soggetti esterni all' Amministrazione.*

Art.5 - Responsabile del trattamento

1. I Responsabili P.O. delle aree funzionali 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 del Comune, Responsabili del trattamento, sono designati 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. E' consentita la nomina di delegati del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento; le operazioni di trattamento possono essere effettuate solo da delegati 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 dei delegati 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 delegato.

4. Il Responsabile del trattamento deve provvedere affinché chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione;

5. 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 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;
- 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. 6 - Responsabile comunale della protezione dei dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato nella figura di un professionista esterno (persona fisica o ditta commerciale) *scelto tramite procedura ad evidenza pubblica*

Il RPD è incaricato dei seguenti compiti:

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 RGPD 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 RGPD 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, può consultare il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

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 può essere invitato a partecipare alle riunioni di coordinamento dei 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 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 collabora, ove richiesto, alla mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

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. 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.

6. 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.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

7. L'atto di nomina ed i dati di contatto del Responsabile comunale della protezione dei dati sono pubblicati sul sito istituzionale del Comune nella sezione *Amministrazione trasparente* e comunicati al Garante della protezione dei dati personali.

8. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi. L'incarico di DPO può essere affidato anche ad un unico soggetto designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D. Lgs. 18 agosto 2000 n. 267.

Art. 7 – Adozione “Registro delle attività di trattamento e delle categorie delle attività”

Al fine di coordinare le attività oggetto di trattamento è adottato il *Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati*”

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 del Comune, del Sindaco e del RPD;
- 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,

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato (Responsabile del trattamento/ P.O. della rispettiva Area) presso gli uffici della struttura organizzativa di competenza del Comune in forma telematica;

3. Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni relative di cui al comma 1 da lett a) a lett. g) e le informazioni delle categorie delle attività trattate, in particolare:

a) 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 personali;

b) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

c) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate,

Art. 8 - Trattamento dei dati personali

1. Le disposizioni del presente regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti del comune comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale il comune provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

2. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti comunali, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.

3. Il responsabile della banca dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 9 – Coordinamento con amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere sia del *Responsabile comunale della protezione dei dati personali* che del *Responsabile Comunale per la prevenzione della corruzione e della trasparenza*, nel caso in cui siano incaricati due soggetti diversi, coordinare la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di pubblicazione dei dati personali in amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale.

2. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la pseudonimizzazione, la minimizzazione e la cifratura dei dati personali.

Art. 10 - Formazione del personale

1. Costituisce onere sia del *Responsabile comunale della protezione dei dati personali* che del *Responsabile Comunale per la prevenzione della corruzione e della trasparenza*, coordinare la loro attività al fine di attuare misure di formazione del personale, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il rispetto delle norme in materia di trasparenza e l'assolvimento degli adempimenti atti a tutelare i diritti di riservatezza dei dati personali dei cittadini e dipendenti.

Art. 11 – Trattamenti consentiti.

1. Il comune, di norma, non è tenuto a chiedere il consenso al trattamento dei dati da parte degli interessati.

2. La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.

3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.

4. Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati oppure utilizzare espressioni di carattere generale, soprattutto nel quadro dell'attività di assistenza e beneficenza, che spesso comporta la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio.

5. Deve essere valutata anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.

6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.

Art. 12 - Principi

1. Negli atti destinati alla pubblicazione o divulgazione i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge, rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

2. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

Art. 13- Attività amministrativa

1. L'attività amministrativa del comune si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.

2. Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni.

3. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse

all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 14. - Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi alla loro nomina, al percorso professionale e ai fatti più significativi che li riguardano, possono mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l'utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati sensibili, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 15 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli

1. Il Comune di Mestrino 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.

Tutta l'attività di gestione è finalizzata a:

- a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
- b) evitare l'accesso, non autorizzato, alle banche dati, alla rete e, in generale, ai servizi informatici del Comune;
- c) prevenire:
 - trattamenti dei dati non conformi alla legge o ai regolamenti;
 - la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

2. I responsabili del trattamento garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, l'adozione e lo sviluppo di misure di sicurezza adeguate come: 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. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.

4. Gli stessi responsabili del trattamento si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.

5. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.(misure di disaster recovery);

6. Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.

Art. 16 – Trattamento e accesso ai dati sensibili e giudiziari

1. Per l'accesso ai dati sensibili e giudiziari, con provvedimento del responsabile del servizio sono rilasciate autorizzazioni a gruppi di lavoro per il trattamento dei dati.

2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all'incaricato.

3. In attuazione del Regolamento UE 2016/679 *le tabelle, raccolte nell'ALLEGATO 1 che formano parte integrante del presente regolamento*, identificano i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite.

4. I dati sensibili e giudiziari individuati dal presente regolamento sono trattati secondo criteri di pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.

5. I dati sensibili o giudiziari non indispensabili, dei quali il comune, nell'espletamento della

propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta del comune medesimo, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 17 - Diritti dell'interessato

1. I soggetti, i cui dati sono contenuti in una banca dati del comune, hanno il diritto di ottenere, senza indugio:

- a) la conferma dell'esistenza o meno di trattamenti di dati che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- c) l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- d) l'attestazione che le operazioni di cui ai successivi commi 2 e 3 sono state portate a conoscenza dei terzi;

2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.

3. L'interessato può esercitare tali diritti con una richiesta al responsabile della banca dati.

4. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 18 – Valutazione 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 o, per conto del medesimo i Responsabili del trattamento, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (**DPIA**) ai sensi dell'art. 35 del Regolamento UE, 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 del Regolamento UE.

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, del Regolamento UE, 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, Regolamento UE;*

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 al Comune. Il Titolare deve consultarsi con il DPO 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 DPO 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 DPO 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, Regolamento UE;*
- *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 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 DPO e che proseguano con le stesse modalità oggetto di tale verifica.

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 Regolamento UE, 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.

Art. 19- Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Il Responsabile del trattamento 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

Art. 20 – Entrata in vigore e normativa applicabile

1. Il presente regolamento entra in vigore con le modalità ed i termini previsti dallo Statuto Comunale;

2. Per quanto non previsto nel presente regolamento trovano applicazione:

- a) le direttive ed i regolamenti comunitari, le leggi nazionali e regionali;
- b) lo statuto comunale;
- c) il regolamento comunale sull'organizzazione generale degli uffici e dei servizi.

Art. 21 - Rinvio dinamico

1. Le norme del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti comunitarie per la parte direttamente applicabile, statali e regionali.

2. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sopraordinata.

Art. 22 - Norme abrogate

1. Con l'entrata in vigore del presente regolamento sono abrogate tutte le norme regolamentari con esso contrastanti.

Art. 23 - Pubblicità del regolamento

1. Copia del presente regolamento è pubblicato nell'apposita sezione di *Amministrazione trasparente* del sito internet istituzionale.

INDICE DELL'ALLEGATO 1:

Tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento

N° scheda	Denominazione del trattamento
1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune
2	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - Attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa
3	Servizi demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
4	Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile
5	Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo
6	Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio
7	Servizi demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari
8	Servizi demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza
9	Servizi demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari
10	Servizi sociali - Attività relativa all'assistenza domiciliare
11	Servizi sociali - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale
12	Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di

	cura, Case di riposo, ecc.
13	Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
14	Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)
15	Servizi sociali - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)
16	Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto o di trasporto sociale.
17	Servizi sociali - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)
18	Servizi sociali - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affidamento e di adozione dei minori
19	Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
20	Servizi sociali - Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario
21	Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne, elementari e medie
22	Istruzione e cultura - Attività di formazione ed in favore del diritto allo studio
23	Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione
24	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica

	sicurezza
25	Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione, nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione
26	Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni
27	Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali
28	Attività riguardante gli istituti di democrazia diretta
29	Attività di protezione civile
30	Conferimento di onorificenze o ricompense
31	Agevolazioni tributarie
32	Attività ricreative, promozione della cultura e dello sport - occupazione di suolo pubblico - uso di beni immobili comunali
33	Iscrizioni ad albi comunali di associazioni ed organizzazioni di volontariato

