

Indirizzi e linee guida di adeguamento al Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

1. TITOLARE E DESIGNATI

Il Comune è l'autorità pubblica titolare del trattamento dei dati ai sensi del Regolamento UE 2016/679 (di seguito GDPR) ed esercita le proprie prerogative, poteri e doveri attraverso gli organi ed il personale dell'Ente secondo le competenze, prerogative e le responsabilità stabilite dalle disposizioni organizzative in materia ed in particolare:

- il Sindaco procede alla designazione e nomina degli organismi monocratici e collegiali previsti dalla normativa e rimessi alla determinazione del titolare con particolare riferimento al DPO (Data Protection Office – Responsabile della protezione dei dati personali), Responsabili esterni, Designati interni, gruppi di lavoro e team di progetto a supporto delle attività specifiche;
- i Responsabili di servizio, 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 Responsabili di servizio ricoprono automaticamente la funzione di organo designato dal Titolare per lo svolgimento delle relative competenze;
- il personale assegnato agli uffici e servizi svolge le funzioni di designato del titolare, senza necessità di ulteriore nomina e/o attribuzione in relazione ai trattamenti ed ai poteri/doveri previsti dal proprio ruolo organizzativo e nel rispetto delle indicazioni formali ed informali disposte dal responsabile del servizio.

2. PRESUPPOSTI DI LICEITÀ DEL TRATTAMENTO

I trattamenti sono compiuti dal Comune di Marcheno sulla base dei seguenti presupposti di liceità:

- 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.La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
- b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
- c) l'esecuzione di un contratto con soggetti interessati;
- d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

3. RESPONSABILI ESTERNI DEL TRATTAMENTO

Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento (ai sensi dell'art. 28 del GDPR), 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.

Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono essere predisposti da ciascun Responsabile interno per le attività di propria competenza. Tali atti devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR.

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 dimostrare che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

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.

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.

4. GRUPPO DI LAVORO GDPR

E' istituito un gruppo di lavoro permanente in materia di adattamento alle norme del GDPR composto da:

- segretario comunale
- responsabili di servizio o uno o più membri designati dai responsabili medesimi in relazione alla competenza, preparazione e/o ruolo nel trattamento di dati particolari
- Il DPO può partecipare al gruppo di lavoro ogni qualvolta lo reputi opportuno.

Le riunioni del gruppo sono tracciate.

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.

5. RESPONSABILIZZAZIONE E REGISTRO DEGLI EVENTI

Il titolare ed i designati assicurano in ogni momento il rispetto dei principi previsti dal GDPR (art. 5) dettando le opportune disposizioni organizzative e procedurali in ogni fase dell'attività.

Il titolare ed i designati assicurano in particolare il rispetto del principio di responsabilizzazione comprovando l'adozione di tali misure mediante la redazione ed aggiornamento di un registro degli eventi nel quale annotare tempestivamente ogni attività svolta per l'attuazione delle disposizioni del GDPR.

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 e dell'autorità di controllo.

Ogni operazione, registrazione, documentazione che necessiti di essere approvata nel rispetto dei principi indicati sarà formalizzata, ove necessario, mediante protocollazione senza necessità di ulteriori formalizzazioni ove non necessarie ai sensi della vigente normativa.

6. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Gruppo di lavoro cura la redazione e coordina l'aggiornamento del registro delle attività di trattamento di cui all'art. 30 del GDPR, mediante acquisizione dai responsabili dei servizi di dati e informazioni sulle tipologie di trattamento, secondo il modello opportunamente predisposto.

Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi.

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 e dell'autorità di controllo.

Il registro, depurato di eventuali informazioni non necessarie o che possano mettere a rischio la sicurezza dell'Ente è pubblicato in rete civica nella sezione dedicata al GDPR.

7. VALUTAZIONE D'IMPATTO

Il Gruppo di lavoro cura la redazione e coordina l'aggiornamento della valutazione d'impatto di cui agli artt. 35-36 del GDPR, mediante acquisizione dai responsabili dei servizi di dati e informazioni sulle tipologie di trattamento, secondo il modello opportunamente predisposto.

Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi.

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 e dell'autorità di controllo.

8. PRINCIPIO DI COLLABORAZIONE

Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:

- collabora con il titolare, il DPO-RPD, l'autorità di controllo ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal GDPR
- fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del GDPR (cosiddetto "data breach")
- collabora con i responsabili del trattamento, secondo le istruzioni fornite dal titolare, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza.

Il rispetto dei principi in materia e dei compiti ed adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto.

9. VIOLAZIONE DI DATI PERSONALI

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'Ente.

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.

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).

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 verificatasi. 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).

