COMUNE DI DRENCHIA

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

ADOTTATO CON DELIBERAZIONE GC n. 31 del 18/05/2018

Art. 1 – Oggetto del Regolamento.

1. Il presente Regolamento 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 (denominato Reg.UE nei successivi articoli) e dei provvedimenti generali adottati dal Garante per la protezione dei dati personali; è conseguentemente abrogato il Regolamento per la tutela della riservatezza nel trattamento di dati personali adottato con deliberazione del Consiglio comunale n. 27 del 23/04/2001.

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. Il presente Regolamento potrà essere oggetto di aggiornamento in relazione all'evoluzione normativa della materia, alle disposizioni dettate dal Garante per la protezione dei dati personali ed alle modifiche organizzative dell'Ente.

4. 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.

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 Drenchia 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. La persona fisica rappresentante del titolare ai fini della normativa in materia di trattamento dei dati personali è il Sindaco, legale rappresentate dell'Ente. Il Sindaco affida al Segretario comunale, quale incarico amministrativo di vertice, il coordinamento e la vigilanza circa il rispetto della normativa in materia di privacy all'interno dell'Ente.

3. Il Segretario comunale:

- si relaziona direttamente con i responsabili della protezione dei dati di cui all'art.7, 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;
- può attivare forme di verifica circa il rispetto, da parte degli uffici, delle norme e disposizioni in materia di trattamento dei dati personali;
- svolge gli ulteriori atti ed attività previste nel presente Regolamento.

Art. 3 – Contitolare del trattamento dei dati.

1. Qualora sia individuabile un soggetto contitolare, insieme al Comune, del trattamento ai sensi dell'art.26 del Reg.UE, i rispettivi ruoli ed obblighi per gli aspetti concernenti il trattamento dei dati devono essere regolati all'interno di un accordo/protocollo/contratto.

2. Presupposto per la contitolarità è la condivisione tra diversi titolari delle finalità e dei mezzi del trattamento dei dati personali.

Art. 4 – Responsabili del trattamento dei dati.

1. Ai sensi degli artt.4 punto 8) e 28 del Reg.UE, i responsabili del trattamento dei dati per conto del Comune sono designati 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. Possono essere designati responsabili del trattamento i soggetti che per esperienza, capacità ed affidabilità forniscano le garanzie previste dalla predetta norma.

Art. 5 – Ruolo dei Dirigenti/Responsabili di Area all'interno del Comune.

1. All'interno dell'organizzazione del Comune i Dirigenti/Responsabili di Area, assegnatari di risorse umane, strumentali e finanziarie, nonché soggetti dotati di competenze gestionali, presidiano all'interno dell'Area assegnata il rispetto della normativa in materia di trattamento di dati personali. A tal fine sono individuati Responsabili per il trattamento dei dati i Dirigenti/Responsabili di Area senza alcun altro apposito atto.

Art. 6 – Soggetti autorizzati al trattamento dei dati.

1. Tutti i dipendenti od 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 Dirigente/responsabile di Area, ai sensi dell'art. 4 punto 10) del Reg.UE ("persone autorizzate al trattamento").

2. In relazione all'organizzazione dell'Area, alle funzioni svolte ed alla tipologia di trattamenti e di dati trattati, il Dirigente/responsabile di Area 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.

3. Tra i soggetti autorizzati al trattamento può essere individuato un "referente privacy" di Area.

Art. 7 – Amministratori di sistema.

1. Le funzioni di "amministratore di sistema", nei diversi profili funzionali previsti, sono attribuite per iscritto dal Dirigente/Responsabile cui afferiscono i servizi informatici, sentito il Titolare.

2. Il predetto Dirigente/Responsabile:

- presidia e controlla l'introduzione e l'attuazione delle misure minime di sicurezza ICT per le pubbliche amministrazioni avvalendosi dell'Amministratore di sistema nominato ed evidenziando al Titolare le necessità di programmazione dei relativi investimenti necessari;
- fornisce ai dipendenti dell'Ente periodiche indicazioni operative per la salvaguardia della sicurezza informatica (a titolo esemplificativo 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.

1. Il responsabile della protezione dei dati, di cui agli artt.37-38-39 del Reg.UE, è designato con provvedimento del Segretario comunale, tenendo presente i requisiti del ruolo indicati nelle predette norme e specificandone i compiti nell'ambito di gestione del servizio, sorveglianza e contatto con il Garante previste dalle predette norme. Detta figura opera in autonomia ed indipendenza, relazionandosi direttamente con il Segretario comunale.

2. 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),.

3. Il servizio di Responsabile della protezione dei dati può comprendere anche iniziative di formazione rivolte ai dipendenti dell'Ente.

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 Dirigente/Responsabile di Area preposto alla gestione dei sistemi informativi.

4. 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 affidamento, che vengono svolti in interlocuzione e confronto con i singoli responsabili del trattamento nominati.

5. Il responsabile della protezione dei dati incaricato ha l'obbligo di astenersi nel caso sussistano condizioni di conflitto di interesse.

Art. 9 – Registri delle attività di trattamento.

1. Il registro di cui all'art.30 del Reg.Ue del titolare del trattamento, contenenti le informazioni minime ivi previste, è distinto in sezioni. L'ambito della singola sezione fa riferimento all'area assegnata al Dirigente/Responsabile

2. Le singole sezioni vengono tenute aggiornate, con nuova protocollazione del documento, in relazione ad eventuali modifiche delle attività di trattamento.

Art. 10 – Valutazione di impatto sulla protezione dei dati.

1. La valutazione di impatto di cui all'art.35 del Reg.UE, previa analisi dei rischi nei trattamenti, viene predisposta nei casi e con le modalità previsti dalla stessa norma e secondo le specifiche fornite dall'Autorità di controllo (Garante privacy), qualora il rischio potenziale del trattamento sia elevato.

2. La valutazione, da effettuare a livello della singola unità organizzativa, è predisposta e sottoscritta, in formato digitale, dal singolo Dirigente/Responsabile di area.

3. Il documento, redatto in collaborazione con il responsabile della protezione dei dati, si basa sulla valutazione dei pericoli per la riservatezza ed i diritti fondamentali della persona e contiene la previsione delle azioni e delle misure di sicurezza e di garanzia per il miglioramento delle condizioni di trattamento e per la mitigazione del rischio.

4. Le singole valutazioni di impatto vengono tenute aggiornate, con nuova protocollazione del documento, in relazione ad eventuali modifiche delle attività di trattamento.

Art. 11 – 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 o 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 specificatele 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. 12 - Misure di sicurezza.

1. I responsabili del trattamento dei dati 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.
2. Con apposito documento, predisposto e sottoscritto in formato digitale, vengono individuate le misure di sicurezza adottate in ambito informatico; tale documento, per il carattere di riservatezza del medesimo, è sottratto alla pubblicazione ed all'accesso da parte di terzi soggetti.
3. Il Segretario generale, sentito il responsabile per la protezione dei dati, può adottare codici di condotta per il trattamento dei dati personali.

Art. 13 – 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/Responsabile di area al Segretario generale 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 generale, consultato preventivamente il responsabile della protezione dei dati, effettua la notifica della violazione all'Autorità di controllo (Garante privacy) e, ove previsto, agli interessati dal trattamento (persone fisiche a cui si riferiscono i dati oggetto di violazione); il Segretario generale 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. 14 – Informativa agli interessati.

1. I Dirigenti/Responsabili di Area curano, all'interno delle aree 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 / p.o. per ottemperare alle finalità di cui alle predette norme.

3. La scelta dei mezzi attraverso cui rendere l'informativa viene valutata dal Dirigente/Responsabile di Area 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 aree. I Dirigenti/Responsabili di area 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. 15 – 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 generale.