



Comune di Salcedo

Provincia di Vicenza

DECRETO N. 4 del 16-02-2026

Oggetto: Designazione ed autorizzazione al trattamento dei dati personali, ai sensi dell'art. 29 Regolamento UE 679/2016 e dell'art. 2-quaterdecies D.lgs. n. 196/2003 Responsabile dell'Area Affari Generali, Servizi alla Popolazione ed Economico Finanziari Maria Chiara Dalla Valle

in qualità di rappresentante legale del Comune di Salcedo, e Titolare del trattamento,

PREMESSO:

che è in vigore il Regolamento (UE) 679/16 del Parlamento Europeo e del Consiglio 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*” (“Regolamento generale sulla protezione dei dati”, di seguito “GDPR”);

che ai sensi dell’art. 29 GDPR chiunque agisca sotto l’autorità del Titolare del trattamento che abbia accesso a dati personali non li può trattare se non è istruito in tal senso dal Titolare del trattamento;

che l’art. 2 quaterdecies del D.lgs. n. 196/2003 (“*Codice in materia di protezione dei dati personali*”, di seguito “*Codice Privacy*”) prevede che il Titolare del trattamento possa prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operino sotto la sua autorità;

che l’art. 32, comma 4, GDPR, prevede che il Titolare del trattamento faccia in modo che chiunque agisca sotto la sua autorità e che abbia accesso ai dati debba essere debitamente istruito sulle modalità di trattamento;

CONSIDERATO il principio di “*Accountability*” (c.d. “responsabilizzazione”) che caratterizza il GDPR, ricavabile in particolare dall’articolo 5, comma 2, e dall’articolo 24 GDPR, di cui il presente atto costituisce espressa applicazione;

RITENUTO necessario individuare all'interno dell'Amministrazione Comunale i soggetti che per esperienza, ruolo, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni di legge in materia di trattamento dei dati, anche sotto il profilo della sicurezza;

VALUTATO che la rag. Maria Chiara Dalla Valle, nominata Responsabile dell'Area Affari Generali, Servizi alla Popolazione ed Economico Finanziari con decreto del Sindaco n. 02/2024 in data 12/06/2024, sia in possesso dei requisiti sopra indicati;

DECRETA

Di designare ed autorizzare la **rag. Maria Chiara Dalla Valle** al trattamento dei dati personali nell'ambito dell'incarico di Responsabile dell'Area Affari Generali, Servizi alla Popolazione ed Economico Finanziari di Salcedo, nel rispetto delle funzioni attribuite e delle istruzioni contenute nel presente atto di designazione.

In qualità di designato ex art. 2 *quaterdecies* Codice Privacy ed autorizzato al trattamento ex art. 29 GDPR, dovrà:

- trattare i dati rispettando le istruzioni impartite dal Titolare, anche ulteriori rispetto alla presente nomina, anche di volta in volta verbalmente espresse, nonché le istruzioni impartite dal Responsabile della Protezione dei dati (di seguito anche solo "DPO") del Comune;
- rispettare il GDPR, il Codice Privacy, i provvedimenti del Garante per la protezione dei dati personali e tutta la normativa in materia di protezione dei dati personali nelle operazioni di trattamento dati, assicurandosi che i dati vengano trattati in conformità alle finalità specifiche;
- vigilare sul rispetto e sulla corretta applicazione della predetta normativa da parte del personale autorizzato del Comune, comunicando al Titolare del trattamento e al Responsabile della Protezione dei dati (di seguito "DPO") gli eventuali nuovi trattamenti da svolgere, provvedendo alle necessarie misure di sicurezza;
- tenere traccia del percorso logico e delle motivazioni che hanno comportato una determinata scelta in materia di privacy;
- verificare periodicamente, con il supporto del DPO e dei Responsabili di Area, l'adeguatezza delle misure di sicurezza adottate, valutando il livello di rischio inerente al trattamento e l'eventuale necessità di adottare misure più adeguate, di concerto con il Titolare del trattamento e con il DPO;
- interagire con i soggetti incaricati di eventuali verifiche, controlli e ispezioni, evadendo tempestivamente le richieste di informazioni da parte dell'Autorità Garante, dando immediata esecuzione alle eventuali indicazioni che pervengano dall'Autorità stessa.

L'autorizzato potrà, pertanto, trattare:

- dati personali comuni;
- dati particolari ai sensi dell'art. 9 GDPR;
- dati relativi a condanne penali e reati ex art. 10 GDPR

degli interessati per le finalità del proprio incarico.

L'autorizzato potrà eseguire tutte le operazioni di trattamento necessarie allo svolgimento dei processi, procedimenti, attività, compiti e funzioni di competenza del proprio ruolo, in base all'organigramma in atto ed alla propria qualifica funzionale.

In particolare, l'autorizzato avrà accesso alle banche dati ed agli archivi il cui accesso è necessario allo svolgimento delle proprie mansioni.

Il trattamento di dati personali sarà effettuato sia con modalità cartacee sia con l'ausilio di strumenti elettronici, nel rispetto delle misure di sicurezza sotto specificate.

ISTRUZIONI DA SEGUIRE NELLE OPERAZIONI DI TRATTAMENTO DATI

In ottemperanza all'art. 5 GDPR, i designati sono tenuti a:

- trattare i dati solo per le finalità istituzionali del Comune indicate negli atti di informazione ex art. 13 -14 GDPR (principio di *“liceità, correttezza e trasparenza”* e di *“limitazione della finalità”*);
- trattare solamente i dati necessari e pertinenti rispetto alle finalità perseguite nell'attività a cui i designati sono preposti (principio di *“minimizzazione dei dati”*);
- assicurare l'esattezza dei dati, rettificando i dati inesatti rispetto alle finalità perseguite (principio di *“esattezza”*);
- assicurarsi che i dati vengano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di *“limitazione della conservazione”*);
- rispettare le misure di sicurezza informatiche, logistiche, procedurali stabilite dal Comune, al fine di evitare trattamenti non autorizzati o illeciti, perdita di dati, distruzioni o danni accidentali (principio di *“integrità e riservatezza”*).

In ogni caso, i designati:

- devono sempre tenere un comportamento tale da garantire la dovuta riservatezza ai dati trattati, da non pregiudicarne in alcun modo l'integrità, da non effettuare o consentire accessi non autorizzati ai dati, trattamenti non consentiti di dati o, comunque, trattamenti non conformi alle finalità della raccolta. È vietata qualsiasi comunicazione o diffusione di dati personali non autorizzata o effettuata al di fuori dei casi previsti dalle leggi applicabili;
- non devono accedere a tipologie di dati personali e di trattamenti diversi da quelli strettamente pertinenti alle mansioni svolte;
- non devono procedere alla creazione di nuovi ed autonomi trattamenti e/o banche dati con finalità diverse da quelle caratterizzanti l'Area di appartenenza, senza preventiva autorizzazione del Titolare;
- devono segnalare tempestivamente al Titolare qualsiasi circostanza pregiudizievole del corretto trattamento di dati personali di cui dovessero venire a conoscenza, affinché possano essere assunti, senza ritardo, gli opportuni provvedimenti correttivi;
- non devono procedere alla raccolta di dati personali se non nell'ambito delle finalità proprie dell'Area di appartenenza;

- in caso di riscontro di una violazione di dati personali (c.d. *Data Breach*), devono comunicare immediatamente la violazione al titolare del trattamento o ai soggetti indicati nel “*Protocollo aziendale sul Data Breach*”, in modo da attivare le procedure previste dagli articoli 33 e seguenti GDPR.

Considerato che il non corretto utilizzo sia degli strumenti informatici e telematici istituzionali, sia della documentazione cartacea prodotta e conservata nell’ambito dello svolgimento delle proprie mansioni, rappresenta una potenziale criticità per la sicurezza dei dati personali degli interessati, i designati al trattamento sono tenuti ad osservare scrupolosamente le seguenti istruzioni.

Trattamento con l’ausilio di strumenti elettronici

Nel trattamento di dati personali effettuato con l’ausilio di strumenti elettronici, i designati al trattamento sono tenuti a rispettare le seguenti istruzioni:

Utilizzo del personal computer in dotazione:

- osservare le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita anche accidentale di dati, accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità del trattamento;
- accedere solo alle cartelle di rete ed alle banche dati inerenti alla propria qualifica;
- non lasciare in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento di dati;
- in caso di allontanamento dalla propria postazione, bloccare il proprio strumento informatico o attivare lo screen saver con password;
- al termine della giornata lavorativa, o in caso di assenza prolungata dal posto di lavoro, spegnere il computer;
- non lasciare mai incustoditi eventuali notebook fuori dalla sede del Comune. Le credenziali di autenticazione non devono essere conservate nella stessa borsa contenente il notebook.

Utilizzo delle credenziali di autenticazione:

- conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- non divulgare a terzi le proprie credenziali di autenticazione, né renderle accessibili a terzi mediante riproduzione su post-it o altri fogli collocati in prossimità dei computer;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno 8 (otto) caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili agli autorizzati;

- prestare attenzione a non essere osservati durante la digitazione della password o di qualunque altro codice di accesso;
- modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo, ed in seguito secondo la scadenza prevista dagli strumenti di regolamentazione interni al Comune (sei mesi in caso di trattamento di dati personali comuni, tre mesi in caso di trattamento di dati particolari).

Gestione dei supporti di memorizzazione:

- tutte le informazioni devono essere salvate sempre e soltanto nelle cartelle di rete presenti nei server del Comune;
- rispettare le procedure per il salvataggio periodico di dati regolamentate dal Comune;
- assicurarsi che i dispositivi di memorizzazione di massa esterni agli strumenti elettronici eventualmente utilizzati siano adeguatamente configurati dal punto di vista della sicurezza, in modo da evitare rischi di accessi non autorizzati ai dati personali;
- eliminare i supporti di memorizzazione in maniera sicura, rendendoli previamente inutilizzabili.

Utilizzo del telefono, della stampante e della fotocopiatrice:

- è proibito discutere, comunicare o trattare dati personali per telefono, se non si è certi che il destinatario sia un soggetto autorizzato a poter trattare i dati in questione. È opportuno evitare di parlare ad alta voce in presenza di terzi non autorizzati, per evitare che questi possano prendere conoscenza, anche accidentale, dei dati, soprattutto durante gli orari di apertura al pubblico degli uffici comunali;
- deve essere limitato l'utilizzo di copie fotostatiche, in modo da evitare il rischio di diffusione di dati;
- nel caso vi siano fotocopiatori collocati in aree accessibili al pubblico, prelevare le copie effettuate nel più breve tempo possibile, evitando di lasciarle incustodite, fermo restando che i fotocopiatori devono essere bloccati nella fuoriuscita di stampa diretta se non sia presente l'operatore che ha stampato il documento;
- non utilizzare copie fotostatiche di documenti di identità (anche se non perfettamente riuscite) come carta riciclata;
- i fogli contenenti dati personali non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da rendere non intelligibili a terzi i dati personali ivi contenuti, usando eventualmente un dispositivo distruggi documenti;
- la fotoreproduzione di documentazione cartacea contenente dati personali deve avvenire a cura delle persone autorizzate a trattare tali dati.

L'autorizzato al trattamento deve osservare le prescrizioni contenute nel "*Regolamento sull'utilizzo degli strumenti informatici e sulla posta elettronica istituzionale*", consegnato a tutto il personale del Comune.

Trattamento senza l'ausilio di strumenti elettronici:

Nel trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici, i designati sono tenuti a rispettare le seguenti istruzioni:

- controllare e custodire gli atti e i documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento;
- le cartelle ed i fascicoli di lavoro devono essere tenuti nella propria scrivania facendo attenzione che i dati eventualmente riportati sul frontespizio non siano visibili a persone non autorizzate;
- in caso di trattamento di dati particolari e di dati relativi a condanne penali e a reati tutta la documentazione cartacea deve essere custodita con estrema cura e conservata in armadi/cassetti chiusi a chiave, le quali devono essere custodite da personale autorizzato (accesso selezionato);
- i documenti contenenti dati personali particolari e dati relativi a condanne penali e a reati, prelevati dall'archivio, devono essere controllati e custoditi dagli autorizzati in maniera che ad essi non accedano persone prive di autorizzazione e devono essere restituiti all'archivio al termine delle operazioni affidate;
- i documenti contenenti dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali; in questo caso, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- per tutto il periodo in cui i documenti contenenti dati personali sono al di fuori dei locali individuati per la loro conservazione, o addirittura all'esterno del luogo di lavoro, il designato non dovrà mai lasciarli incustoditi e dovrà sempre tenere con sé la cartella o la borsa nella quale i documenti sono contenuti;
- controllare che i documenti contenenti dati personali composti da numerose pagine o più raccoglitori siano sempre completi ed integri;
- al termine dell'orario di lavoro, riporre i documenti contenenti dati personali nei locali individuati per la loro conservazione;
- è necessario adottare particolari cautele nel caso in cui vengano consegnati ad altri soggetti autorizzati documenti in originale.

Il presente incarico è efficace per tutta la durata dell'incarico di Responsabile dell'Area Affari Generali, Servizi alla Popolazione ed Economico Finanziari ed è strettamente funzionale e collegato alle mansioni svolte dall'autorizzato/designato e necessario per l'esecuzione delle stesse. Non costituisce, pertanto, conferimento di nuovo ruolo o mansioni.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica e/o cessazione dell'incarico.

L'autorizzato/designato dichiara di aver preso conoscenza dei compiti che gli sono stati affidati.

Composizione del documento:

- Atto dispositivo principale
- Eventuale Certificati ed allegati indicati nel testo

Il Sindaco
Carli Michele

Documento informatico firmato digitalmente ai sensi e con gli effetti del d.lgs n. 82/2005 (CAD) e s.m.i.;e norme collegate; Sostituisce il documento cartaceo e la firma autografa.