COMUNE DI CALENDASCO

PROCEDURA PER L'INQUADRAMENTO DEL RUOLO PRIVACY DEI FORNITORI

Sommario

1. Premessa 2
2. Contesto normativo e regolamentare 3
3. Definizioni 4
4. Ruolo del fornitore ai fini della protezione dei dati personali 4
5. Individuazione del ruolo privacy del fornitore: metodo operativo 5
6. Scelta del fornitore e valutazione ai fini dell'eventuale nomina a Responsabile del trattamento 5
7. Valutazione delle garanzie offerte dal fornitore (art. 28, par. 1, GDPR) 6
8. Indicazione delle informazioni essenziali del trattamento 6
9. Gestione dei sub-responsabili 7
10. Allegati 8
11. Revisione e aggiornamento 8
12. Disposizioni finali 8
Allegato 8

1. Premessa

1.1 La presente policy è adottata da:

COMUNE DI CALENDASCO, con sede in 29010 Calendasco (PC), via G. Mazzini n. 4, codice fiscale 00216710335, in persona del legale rappresentante pro tempore, nella qualità di Titolare del trattamento (di seguito "**Titolare**" o "**Ente**").

1.2 La policy disciplina le modalità di qualificazione giuridica, ai fini della protezione dei dati personali, dei soggetti terzi con cui l'Ente instaura rapporti contrattuali nell'ambito dello svolgimento delle proprie attività istituzionali e che, in ragione delle prestazioni affidate, possono effettuare operazioni di trattamento di dati personali.

1.3 In particolare, la presente policy definisce i criteri e le modalità attraverso cui l'Ente provvede a:

valutare il ruolo dei soggetti terzi coinvolti nel trattamento di dati personali (es. Responsabile del trattamento, Titolare autonomo o Contitolare);

formalizzare i rapporti di trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR), ove ne ricorrano i presupposti;

impartire istruzioni documentate ai soggetti nominati Responsabili del trattamento;

garantire il rispetto del principio di responsabilizzazione (accountability) di cui all'art. 5, par. 2, GDPR.

1.4 La presente policy si applica a tutti i soggetti dell'Ente coinvolti, a vario titolo, nella gestione dei rapporti contrattuali con fornitori o altri soggetti esterni che trattano dati personali per conto dell'Ente.

2. Contesto normativo e regolamentare

2.1 La presente policy è redatta nel rispetto del quadro normativo vigente in materia di protezione dei dati personali e, in particolare, tenendo conto:

- del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("GDPR");
- del D. Lgs. 30 giugno 2003, n. 196, così come modificato ed integrato dal D. Lgs. 10 agosto 2018, n. 101 ("Codice in materia di protezione dei dati personali");
- del D. Lgs. 31 marzo 2023, n. 36 ("Codice dei contratti pubblici"), con riferimento alle procedure di affidamento di servizi che comportano trattamenti di dati personali per conto dell'Ente.

2.2 La policy e i relativi allegati tengono inoltre conto:

- delle "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR" adottate dal Comitato europeo per la protezione dei dati (EDPB);

> dei provvedimenti e delle Linee guida adottati dal Garante per la protezione dei dati personali.

3. Definizioni

3.1 Salvo quanto diversamente previsto nel presente documento, si rinvia alle definizioni contenute nel MOP adottato dall'Ente.

3.2 Ai fini della presente policy si intende per:

> **fornitore**: qualsiasi soggetto esterno all'organizzazione con cui l'Ente instaura un rapporto contrattuale per la fornitura di beni o servizi e che, nello svolgimento delle attività affidate, può trovarsi a trattare dati personali per conto dell'Ente;

> **sub-responsabile del trattamento**: soggetto terzo di cui il Responsabile del trattamento si avvale per l'esecuzione di specifiche attività di trattamento per conto del Titolare, previa autorizzazione scritta di quest'ultimo ai sensi dell'art. 28 del GDPR;

> **atto di nomina a Responsabile del trattamento**: atto giuridico, ai sensi dell'art. 28 del GDPR, che disciplina le operazioni di trattamento effettuate dal fornitore per conto dell'Ente;

> **audit**: attività di verifica periodica volta a valutare la conformità del Responsabile del trattamento alle istruzioni impartite dal Titolare e alle disposizioni normative applicabili.

4. Ruolo del fornitore ai fini della protezione dei dati personali

4.1 Nell'ambito del processo di selezione e contrattualizzazione dei fornitori, l'Ente valuta preliminarmente il ruolo che il soggetto esterno ricopre rispetto ai trattamenti di dati personali connessi alle attività affidate.

4.2 In particolare, l'Ente verifica se il fornitore:

> tratti dati personali per conto dell'Ente e sulla base di istruzioni documentate, configurandosi quale Responsabile del trattamento ai sensi dell'art. 28 del GDPR; oppure

> determini autonomamente le finalità e i mezzi del trattamento connesso alle attività svolte, configurandosi quale Titolare autonomo.

4.3 La qualificazione del ruolo del fornitore tiene conto della natura delle attività affidate e del grado di autonomia decisionale riconosciuto allo stesso nello svolgimento del trattamento, anche alla luce delle disposizioni normative applicabili a specifiche categorie professionali o settoriali.

4.4 La corretta individuazione del ruolo del fornitore costituisce presupposto per la definizione dell'assetto contrattuale e delle misure organizzative da adottare ai fini della protezione dei dati personali.

5. Individuazione del ruolo privacy del fornitore: metodo operativo

5.1 Al fine di supportare la qualificazione del ruolo del fornitore ai fini della protezione dei dati personali, l'Ente si avvale di una checklist operativa contenente una serie di domande guida (**allegato 1**), finalizzate a valutare il grado di autonomia decisionale del fornitore rispetto alle finalità e ai mezzi del trattamento.

5.2 Le risultanze della checklist costituiscono uno strumento di supporto alla valutazione, ma non determinano automaticamente la qualificazione del ruolo del fornitore, che deve essere effettuata sulla base di un'analisi complessiva delle attività affidate e delle modalità concrete di svolgimento del trattamento.

5.3 Qualora il fornitore tratti dati personali esclusivamente per conto dell'Ente e sulla base di istruzioni documentate, lo stesso è qualificato quale Responsabile del trattamento ai sensi dell'art. 28 del GDPR.

5.4 Nei casi in cui il fornitore determini autonomamente le finalità e i mezzi del trattamento connesso alle attività svolte, lo stesso è qualificato quale Titolare autonomo.

5.5 In situazioni residuali, da valutare caso per caso, può configurarsi un'ipotesi di contitolarità del trattamento ai sensi dell'art. 26 del GDPR, qualora due o più soggetti determinino congiuntamente le finalità e i mezzi del trattamento.

6. Scelta del fornitore e valutazione ai fini dell'eventuale nomina a Responsabile del trattamento

6.1 Una volta individuato il fornitore nell'ambito del rapporto contrattuale e definito il relativo ruolo ai fini della protezione dei dati personali, qualora lo stesso risulti operare quale Responsabile del trattamento, l'Ente procede alla valutazione delle garanzie di cui all'art. 28 del GDPR.

6.2 In attuazione del principio di responsabilizzazione (accountability), l'Ente è tenuto a selezionare esclusivamente soggetti che presentino garanzie sufficienti in termini di conoscenze specialistiche, affidabilità e capacità di mettere in atto misure tecniche e organizzative adeguate, tali da assicurare che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.

6.3 A tal fine, il processo prevede:

- la verifica dei requisiti del fornitore, mediante acquisizione e valutazione di informazioni e documentazione rilevante (es. policy interne, certificazioni, attestazioni, esiti di audit o altri elementi utili);
- la formalizzazione del rapporto ai sensi dell'art. 28 del GDPR, mediante la stipula di un atto di nomina a Responsabile del trattamento integrato nel contratto principale o ad esso allegato, contenente le istruzioni documentate impartite dall'Ente.

6.4 L'atto di nomina a Responsabile del trattamento può essere proposto dal fornitore, fermo restando il potere dell'Ente di verificarne il contenuto ed eventualmente richiederne modifiche o integrazioni, al fine di assicurarne la conformità alla normativa applicabile.

7. Valutazione delle garanzie offerte dal fornitore (art. 28, par. 1, GDPR)

7.1 Qualora il fornitore sia qualificato quale Responsabile del trattamento, l'Ente valuta, prima della relativa nomina, che lo stesso presenti garanzie sufficienti in termini di affidabilità e capacità di mettere in atto misure tecniche e organizzative adeguate ai sensi dell'art. 28, par. 1, del GDPR.

7.2 Tale valutazione è effettuata tenendo conto della natura delle attività affidate, della tipologia di dati personali trattati e dei rischi connessi al trattamento, anche sulla base delle informazioni rese disponibili dal fornitore nell'ambito della procedura di affidamento o di esecuzione contrattuale.

7.3 Nei casi in cui il trattamento presenti rischi particolari per i diritti e le libertà degli interessati, l'Ente può acquisire ulteriori informazioni o documentazione idonea a comprovare l'adozione di misure tecniche e organizzative adeguate.

7.4 L'Ente assicura che, per tutta la durata del rapporto contrattuale, il trattamento dei dati personali da parte del Responsabile avvenga nel rispetto delle istruzioni impartite e delle condizioni previste nell'atto di nomina ai sensi dell'art. 28 del GDPR.

8. Indicazione delle informazioni essenziali del trattamento

8.1 In fase di nomina del fornitore quale Responsabile del trattamento, l'Ente presta particolare attenzione alla definizione puntuale delle informazioni che circoscrivono le operazioni di trattamento affidate, in conformità a quanto previsto dall'art. 28, par. 3, GDPR.

8.2 Tali informazioni devono includere:

- l'oggetto del trattamento (es. servizi di gestione e manutenzione di sistemi informativi comunali, supporto tecnico a software gestionali in uso agli uffici, servizi di conservazione digitale dei documenti amministrativi, gestione di piattaforme per la presentazione di istanze online o per l'erogazione di servizi al cittadino);

- le finalità del trattamento (es. supporto allo svolgimento di procedimenti amministrativi, gestione di servizi istituzionali dell'Ente, manutenzione e assistenza tecnica delle banche dati, erogazione di servizi digitali ai cittadini o alle imprese);
- la durata del trattamento (es. per tutta la durata del contratto di servizio; fino alla cessazione delle attività oggetto di affidamento; per il tempo strettamente necessario all'esecuzione delle prestazioni contrattuali);
- il tipo di dati personali oggetto di trattamento (es. dati anagrafici e identificativi, dati di contatto, dati relativi a procedimenti amministrativi, dati patrimoniali o economici connessi a tributi o benefici, dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR eventualmente trattati nell'ambito dei servizi sociali o scolastici);
- le categorie di interessati cui i dati si riferiscono (es. cittadini, utenti dei servizi comunali, contribuenti, dipendenti e collaboratori dell'Ente, rappresentanti di imprese o professionisti coinvolti in procedimenti amministrativi).

8.3 La corretta formalizzazione di tali elementi è essenziale per garantire che il trattamento venga svolto nei limiti delle istruzioni impartite dall'Ente e per assicurare la tracciabilità e la verifica delle attività svolte dal fornitore.

9. Gestione dei sub-responsabili

9.1 Qualora il Responsabile del trattamento intenda ricorrere a soggetti terzi per l'esecuzione, in tutto o in parte, delle operazioni di trattamento affidate dall'Ente, è tenuto a richiedere una preventiva autorizzazione scritta al Titolare.

9.2 L'autorizzazione dell'Ente può essere:

- specifica, riferita a uno o più sub-responsabili individuati nominativamente;
- generale, con riferimento a una categoria di sub-responsabili, fermo restando l'obbligo per il Responsabile di informare preventivamente l'Ente in merito a eventuali modifiche riguardanti l'aggiunta o la sostituzione di tali soggetti, al fine di consentire al Titolare di opporsi entro un termine ragionevole.

9.3 In caso di ricorso a sub-responsabili, il Responsabile è tenuto a comunicare all'Ente:

- l'identità del sub-responsabile (ragione sociale e recapiti);
- le attività di trattamento che si intendono affidare;
- ogni ulteriore informazione utile a valutare l'adeguatezza del soggetto designato.

9.4 In ogni caso, il Responsabile del trattamento è tenuto a:

- stipulare con il sub-responsabile un contratto o altro atto giuridico vincolante che imponga a quest'ultimo obblighi in materia di protezione dei dati personali equivalenti

a quelli previsti nel rapporto tra l'Ente e il Responsabile, ai sensi dell'art. 28 del GDPR;

- verificare che il sub-responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate;
- non autorizzare il ricorso a ulteriori sub-responsabili senza previa informazione all'Ente e nel rispetto delle modalità di autorizzazione previste;
- rimanere pienamente responsabile nei confronti dell'Ente per l'adempimento degli obblighi del sub-responsabile, anche in caso di coinvolgimento di quest'ultimo nello svolgimento delle operazioni di trattamento.

9.5 L'Ente si riserva la facoltà di opporsi al ricorso a uno o più sub-responsabili ovvero di revocare l'autorizzazione precedentemente concessa qualora non risultino più soddisfatte le garanzie di adeguatezza richieste ai sensi dell'art. 28 del GDPR. In tali casi, il Responsabile è tenuto a cessare il ricorso al sub-responsabile interessato, fatte salve le attività strettamente necessarie alla gestione della cessazione del trattamento.

10. Allegati

10.1 È parte integrante della presente procedura la checklist per la qualificazione del ruolo privacy del fornitore (**allegato)**.

11. Revisione e aggiornamento

11.1 Il presente documento potrà essere revisionato e aggiornato in relazione a mutamenti normativi o organizzativi dell'Ente.

12. Disposizioni finali

12.1 L'Ente provvede alla diffusione del presente documento con le modalità ritenute più opportune.

Allegato

CHECKLIST PER LA QUALIFICAZIONE DEL RUOLO PRIVACY DEL FORNITORE

Introduzione

La presente checklist supporta la corretta individuazione del ruolo privacy del fornitore (Titolare autonomo, Responsabile del trattamento o Contitolare) nell'ambito dell'affidamento di servizi o attività da parte dell'Ente che comportino il trattamento di dati personali. La compilazione può essere effettuata a cura del referente interno competente o del Referente in materia di protezione dei dati personali, ove individuato.

Istruzioni

Per ciascuna delle seguenti affermazioni, barrare la casella corrispondente a seconda che la risposta sia affermativa o negativa. La colonna "Indicazione se Sì" aiuta a comprendere se, in caso di risposta positiva, l'elemento valutato orienta verso la qualifica di Responsabile del trattamento o di Titolare autonomo.

Sezione A – Checklist operativa

N.	Descrizione	Sì	No	Indicazione se "Sì"
1	Il fornitore tratta i dati personali esclusivamente sulla base di istruzioni documentate fornite dall'Ente?	☐	☐	Responsabile
2	Il contratto disciplina in modo puntuale le operazioni di trattamento (finalità, durata, categorie di dati e interessati)?	☐	☐	Responsabile
3	Il fornitore non determina autonomamente le finalità del trattamento?	☐	☐	Responsabile
4	Il fornitore può riutilizzare i dati personali per proprie finalità ulteriori rispetto al servizio affidato?	☐	☐	Titolare
5	L'attività svolta dal fornitore è soggetta a specifici obblighi di legge o codici deontologici che ne determinano l'autonomia (es. avvocati, medici, revisori)?	☐	☐	Titolare
6	Il fornitore determina in autonomia le finalità del trattamento o i mezzi essenziali dello stesso?	☐	☐	Titolare
7	L'Ente conserva il potere di audit e controllo sulle operazioni di trattamento svolte dal fornitore?	☐	☐	Responsabile
8	Il fornitore deve richiedere autorizzazione scritta all'Ente prima di ricorrere a sub-responsabili?	☐	☐	Responsabile

Sezione B – Risultato e interpretazione

> La checklist costituisce uno strumento di supporto alla valutazione del ruolo del fornitore ai fini privacy.

> La qualificazione del fornitore quale Titolare autonomo, Responsabile del trattamento o Contitolare deve essere effettuata caso per caso, sulla base dell'analisi delle modalità concrete di svolgimento del trattamento e, in particolare, della determinazione delle finalità e dei mezzi essenziali dello stesso.

- Le risposte fornite orientano la valutazione, ma non determinano automaticamente la qualificazione del ruolo, che deve essere formalizzata e adeguatamente motivata in sede di stipula del rapporto contrattuale.
- Qualora emerga che le finalità e i mezzi del trattamento siano determinati congiuntamente dall'Ente e dal fornitore, può configurarsi una situazione di contitolarità del trattamento ai sensi dell'art. 26 del GDPR.