

# CAPITOLATO

**OGGETTO DELL'APPALTO:** ADEMPIMENTI DISPOSTI DAL REGOLAMENTO EUROPEO UE 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI NEL COMUNE DI CASTIGLIONE DELLA PESCAIA COMPRENDENTE LO SVOLGIMENTO DEL RUOLO DI RESPONSABILE DELLA PROTEZIONE DATI PERSONALI DI CUI AGLI ARTICOLI 37, 38 E 39 DELLO STESSO REGOLAMENTO.

**DESCRIZIONE DEL SERVIZIO:** La gestione di sistemi complessi, che trattano dati personali particolarmente delicati, richiede un'attenzione assoluta alle modalità con cui tali dati vengono manipolati ed un accentrimento della consapevolezza – e della responsabilizzazione – in merito a questo tema.

L'entrata in vigore del Regolamento Europeo (GDPR - “General Data Protection Regulation”) implica la necessità di svolgere scelte progettuali precise in un'ottica di “Privacy by design”, nel caso di progettazione di nuovi sistemi, ed un'attenta rivalutazione delle scelte procedurali nella gestione quotidiana nonché della necessaria verifica dell'adeguatezza dei sistemi informativi in dotazione nell'Ente .

Infatti, il novellato contesto normativo si basa sul principio di accountability (tradotto in italiano come “responsabilizzazione”) in virtù del quale il titolare del trattamento adotta politiche e attua misure adeguate per garantire – ed essere in grado di dimostrare – che il trattamento dei dati personali effettuato sia conforme a quanto disciplinato dal GDPR (art. 5, par. 2).

A tal fine l'Amministrazione Comunale di Castiglione della Pescaia intende avvalersi di servizi di attività di consulenza, supporto, assistenza, formazione e predisposizione della necessaria modulistica/documentazione volti a introdurre misure strutturali ben determinate che contribuiscano ad ottenere la massima protezione delle informazioni (sia per quanto riguarda i dati personali, sia le informazioni critiche per la propria attività) e la garanzia di continuità di servizio, introducendo una particolare attenzione alle componenti informatiche.

Il servizio è, dunque, finalizzato a garantire la sicurezza, privacy e la conservazione dei dati trattati nel Comune di Castiglione della Pescaia.

## CARATTERISTICHE E MODALITÀ DI SVOLGIMENTO

Il servizio deve articolarsi in una costante attività di consulenza, supporto, assistenza, formazione e predisposizione della necessaria modulistica/documentazione. Inoltre, dovrà essere assicurata la presenza dell'esperto on site di almeno 2 volte al mese (in date ed orari da concordare). Il servizio dovrà anche garantire la disponibilità ad affrontare e risolvere tutte le questioni afferenti al trattamento dei dati di competenza del Responsabile della Protezione Dei Dati mediante contatto telefonico e posta elettronica entro 48 ore dalla ricezione del quesito, salvo che la questione posta non presenti particolare complessità. In caso di attività ispettive promosse dall'Autorità di controllo/Garante, dovrà essere assicurata la presenza presso la sede del Comune, previa preventiva informazione, dell'esperto in materia.

Gli ambiti di intervento su cui dovrà incentrarsi l'attività del servizio risulteranno essere quelli di seguito riportati. Essi risulteranno indicati a titolo puramente esemplificativo e non completamente esaustivo:

## **1. Assessment relative a General Data Protection Regulation (GDPR).**

Si richiede, alla luce di una verifica puntuale dei dati trattati e della loro classificazione, un'indagine esaustiva sulle attuali modalità di trattamento dei dati personali e sulle modalità con cui la Stazione Appaltante li gestisce e li protegge, tenendo conto delle "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" documento emesso dall'Agid il 26 Aprile 2016.

E' richiesta, quindi, una Gap Analysis per contestualizzare la metodologia prevista rispetto alla specifica realtà di intervento, mappandovi i requisiti previsti dal GDPR, e definendo un Piano di allineamento al Regolamento (UE) 2016/679.

L'attività iniziale dovrà prevedere un'ampia rilevazione dell'esistente che necessariamente dovrà verificare la tipologia dei dati trattati dal Comune suddividendoli secondo le classificazioni del Regolamento suddetto, e come gli stessi vengono trattati in base alla normativa attualmente vigente.

Si dovrà poi verificare l'operatività posta in essere dall'Ente in merito al trattamento dei dati e alla raccolta del consenso e se queste sono in linea con la normativa prevista. Risulterà, pertanto, doveroso effettuare una ricognizione e rivedere tutta la filiera del flusso del dato e dei processi aziendali sottostanti;

A seguire dovranno essere individuate, prodotte, attuate ed aggiornate misure tecniche ed organizzative, nonché atti e documenti per garantire che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. A tal fine:

- dovranno essere individuati i soggetti titolari al trattamento dei dati, suddivisi per competenze e ruoli;
- dovranno essere certificate le procedure interne per la raccolta del consenso, per l'informativa e per tutti gli altri adempimenti previsti dalla normativa vigente;
- saranno revisionati o redatti i testi delle informative e dei consensi al trattamento dei dati personali, ed alle logiche di conservazione, così come i testi degli incarichi e delle nomine al trattamento secondo il GDPR;
- dovrà essere redatto il Piano di Valutazione d'impatto sui Dati Personali per quelle situazioni che presentano rischi specifici per i diritti degli utenti interessati e tutte le altre procedure previste, con riguardo in particolare alla Data Breach Notification/Communication Management.

## **2. ICT Assessment (Infrastructure, Applications, Risk Management, Security)**

In questa fase dovrà essere analizzato lo stato attuale della struttura Comunale, valutando nel dettaglio l'organizzazione, i processi presenti, l'infrastruttura fisica e le funzionalità applicative dei sistemi informatici al fine di produrre un inventario delle attività.

Per quanto riguarda la parte Infrastructure & Applications sono richieste:

- le attività di verifica delle Postazioni di Lavoro (sia in termini di sicurezza che di gestione), delle modalità di inventariazione delle componenti ICT;
- dovrà essere verificata la presenza di procedure appropriate per il governo dei processi, ed un'analisi dei criteri di sicurezza degli applicativi dal punto di vista della robustezza e protezione dei dati;
- dovrà essere effettuata una valutazione del processo nella sua completezza, indicandone le falle operative o le carenze;

Per quanto riguarda la Sicurezza, viene richiesta un'analisi del rischio informatico e delle attuali pratiche adottate per la protezione dei dati, incluse le metodologie in uso volte a mitigare

il rischio informatico comprensive delle indicazione delle azioni necessarie per l'adeguamento alle disposizioni AGID in materia di sicurezza informatica.

### **3. Predisposizione di un Regolamento comunale per la Gestione della Privacy**

La necessaria predisposizione ed aggiornamento di un Regolamento che abbia per oggetto misure procedurali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Castiglione della Pescaia.

### **4. Interventi formativi per il personale**

Il GDPR prescrive all'art. 29 che chiunque tratta dati personali deve essere stato istruito dal Titolare. All'art. 32 si fa riferimento a misure tecniche e organizzative che devono essere testate, verificate e valutate. Nella Sezione 4 dedicata al DPO si prescrive che esso deve avere competenze professionali qualificate e deve sorvegliare sulla formazione di tutta l'azienda (*training of staff*, art.39).

Ciò significa che il servizio deve prevedere la realizzazione di costanti processi formativi rivolti a tutti i dipendenti ed agli operatori che trattano dati in servizio presso il Comune di Castiglione della Pescaia.

### **5. Individuazione e nomina DPO**

Il Regolamento 678/2016 (art. 37) prevede l'obbligo per le autorità pubbliche e gli organismi di diritto pubblico di nominare un DPO – Data Protection Officer (in italiano, RPD o responsabile della protezione dei dati personali)

Si tratta di una figura che deve possedere dei requisiti specifici in termini di esperienza e competenza e deve occuparsi prevalentemente di informare e fornire consulenza sulla corretta applicazione della normativa, curando con particolare attenzione della formazione del personale. In particolare deve garantire lo svolgimento dei seguenti compiti:

- a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento Europeo nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b) sorvegliare sull'osservanza e sull'attuazione del Regolamento Europeo, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento Europeo;
- d) cooperare con il garante per la protezione dei dati personali;
- e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento Europeo, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

- f) eseguire i propri compiti considerando debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso;
- g) riferisce al vertice gerarchico del titolare del trattamento o del responsabile del trattamento;

## **6. Nomina dei Responsabili esterni del trattamento, ai sensi dell'art. 28 GDPR.**

La norma prevede espressamente che *“qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato”*.

Di conseguenza, nella consapevolezza che molti dei fornitori tecnologici trattano dati per conto dell'Ente (es. provider, servizi cloud oppure fornitori di servizi di assistenza e manutenzione) sarà importante che le amministrazioni inizino a sceglierli anche in base a tali misure tecniche e organizzative da questi adottate e sulla base del loro livello di adeguamento al GDPR.

Inoltre, i trattamenti da parte di un responsabile esterno del trattamento devono essere disciplinati da un contratto che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

In virtù della delicatezza dei trattamenti posti in essere dai responsabili esterni, non v'è dubbio che la modifica e l'integrazione degli atti di nomina sia una delle priorità delle attività di adeguamento così come l'adeguamento contrattuale dei servizi affidati all'esterno.

A tal fine il servizio dovrà prevedere un'assistenza alla predisposizione contrattuale dei nuovi rapporti con soggetti esterni responsabili del trattamento dati affidatari di servizi così come la verifica capillare e puntuale comprensivo della bonifica eventuale per quelli in essere alla data di entrata in vigore del Regolamento.

## **7. Trasparenza del trattamento**

Il Regolamento 679/2016 prevede un generale dovere di trasparenza del titolare del trattamento che può essere scomposto in due distinti obblighi.

Da un lato la c.d. “trasparenza proattiva” che si sostanzia nell'obbligo per il titolare di rendere l'informativa, cioè di dare evidenza – senza alcuna specifica richiesta – delle principali informazioni che riguardano il trattamento.

Accanto a tale dovere, si affiancano obblighi di “trasparenza reattiva”, vale a dire l'obbligo di riscontrare le richieste di interessato e aventi ad oggetto non solo i dati forniti precedentemente dallo stesso, ma anche gli altri dati che il titolare abbia raccolto da altre fonti.

L'adeguamento al principio di trasparenza impone alle amministrazioni due fronti di lavoro che il presente servizio oggetto di affidamento dovrà prevedere:

- adeguare e integrare le informative attualmente in uso (con riferimento alle informazioni previste dagli artt. 13 e 14 GDPR), facendo attenzione a renderle chiare, brevi e facilmente comprensibili;
- organizzarsi per riscontrare le richieste di accesso nel termine di trenta giorni dalla ricezione.

## **8. Registro dei trattamenti e misure di sicurezza**

Uno dei principali nuovi adempimenti previsto dall'art. 30 del GDPR a cui il servizio deve occuparsi è quello di predisporre entro il 25 maggio 2018 di un registro per ciascuna categoria delle attività di trattamento dati in cui descrivere:

- a. il nome e i dati di contatto del titolare del trattamento e del DPO;
- b. le finalità del trattamento;
- c. una descrizione delle categorie di interessati e delle categorie di dati personali;
- d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- f. una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione;

Infatti, le amministrazioni, come ogni titolare, sono tenute ad adottare misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

## **9. Sistema sanzionatorio**

Il sistema sanzionatorio posto a presidio dell'osservanza del Regolamento prevede sanzioni amministrative elevate (art. 83 GDPR) e la responsabilità civile nei confronti dell'interessato che subisce un danno materiale o immateriale causato da una violazione del Regolamento (art. 82 GDPR).

A tal fine il servizio richiesto deve prevedere un'assistenza completa nell'eventuale cooperazione con l'Autorità di controllo/Garante notificando qualsiasi violazione dei dati personali allo stesso e al diretto interessato (art. 32-34) entro le 72 ore di tempo nonché nella notifica ai soggetti coinvolti delle violazioni dei dati personali, i cosiddetti Data Breach.

## **10. Diritto all'oblio**

Assistenza e consulenza relativamente ai tre diversi articoli del Regolamento GDPR (articoli 17, 18 e 19). In particolare per quanto concerne l'articolo 17 il quale esplicita quale siano le condizioni che consentono all'interessato di richiedere la cancellazione di dati e informazioni presenti online. I dati, infatti, devono essere cancellati se non sono più necessari ai fini del trattamento per i quali sono stati raccolti, se l'interessato revoca l'autorizzazione, se c'è opposizione dell'interessato al trattamento dei dati, se un tribunale ne ordina la cancellazione e se sono stati trattati illegalmente.

**PERIODO DI SVOLGIMENTO:** durata di 2 anni dalla data di stipula del contratto.

**COSTO DEL SERVIZIO:** corrispettivo pari a circa € 3.675,00 annuo, escluso IVA. Per un totale complessivo di euro 7.350,00 escluso IVA

**REQUISITI:**

1. il possesso di iscrizione al Registro delle Imprese tenuto dalla Camera di Commercio Industria Artigianato Agricoltura società cooperative o, per i Consorzi di cui all'art. 48 del D.Lgs. n. 50/2016, di essere iscritta all'Albo nazionale Enti Cooperativi (D.Lgs. 220/2002);

2. requisiti di ordine generale di cui all'art. 80 del D.Lgs n. 50/2016;

Non sarà ammesso il subappalto o il sub affidamento, totale o parziale, delle prestazioni oggetto del contratto a pena di risoluzione del medesimo.

**CRITERIO DI AGGIUDICAZIONE:** Essendo il valore del servizio inferiore a € 40.000,00 (euro quarantamila/00) iva esclusa, si procederà all'individuazione dell'affidatario mediante affidamento diretto adeguatamente motivato ai sensi dell'art. 36 comma 2, lettera a) del D. Lgs. n. 50 del 18.04.2016.

**MODALITÀ DI PAGAMENTO**

L'Ente si impegna a corrispondere alla Ditta Affidataria un importo complessivo pari a circa € 8.979,20, incluso IVA.

Tale importo verrà suddiviso in quattro semestralità e liquidato previa rendicontazione e presentazione di idonee fatture.

La ditta affidataria del servizio emetterà fattura digitale intestata a "Comune di Castiglione della Pescaia" codice univo di fatturazione Uff. Segreteria: 5GWEAS.

Le fatture emesse saranno liquidate entro 30 giorni dalla data di ricevimento. La Ditta affidataria dovrà assumere gli obblighi di tracciabilità dei flussi finanziari previsti dall'art. 3 della legge 13/8/2010, n. 136, ed in particolare dovrà utilizzare uno o più conti correnti dedicati, anche in via non esclusiva, accesi presso banche o presso la società Poste Italiane SpA, effettuando tutti i movimenti finanziari relativi all'appalto su detti conti correnti mediante bonifico bancario o postale riportante il CIG, fatto salvo quanto previsto all'art. 3, comma 3, della legge citata.

**ESONERO DELLE RESPONSABILITÀ DA PARTE DEL COMUNE**

L'aggiudicatario assume la responsabilità nei confronti del Comune di Castiglione della Pescaia e dei terzi dei danni di qualsiasi natura, materiali o immateriali, diretti ed indiretti, causati a cose o persone e connessi all'esecuzione del contratto, anche se derivanti dall'operato dei suoi dipendenti e consulenti. E' fatto obbligo all'aggiudicatario di mantenere il Comune manlevato da richieste di risarcimento dei danni e da eventuali azioni legali promosse da terzi.

**PENALITÀ**

Nel caso in cui, per qualsiasi motivo imputabile alla società, il servizio non sia conforme a quanto previsto dal contratto e/od in caso di mancato espletamento di supporto, sostegno ed intervento a seguito di documentata richiesta, inviata in via telematica, nel tempo massimo di 48 ore, l'Amministrazione applicherà una penale di € 50,00 per ogni giorno di ritardo relativo alla procedure di intervento richieste .

Delle applicazioni delle eventuali penali e dei motivi che le hanno determinate, il Dirigente Responsabile od il Responsabile Ufficio Servizi alla Persona renderà informata la società con PEC.

**FORO COMPETENTE**

Per ogni controversia, è competente il Foro di Grosseto.

L'insorgere di un eventuale contenzioso non esime comunque la Ditta dall'obbligo di eseguire le prestazioni contrattuali.

**SPESE CONTRATTUALI**

La presente convenzione sarà registrata solo “in caso d’uso”, a semplice richiesta di una delle parti.  
Le spese contrattuali, comunque inerenti e conseguenti, sono assunte per intero dalla Ditta affidataria.