ALLEGATO 3

ACI - Automobile Club d'Italia

Capitolato tecnico e prestazionale

PROCEDURA APERTA TELEMATICA N. 1/2023 DTAPDRP PER L'AFFIDAMENTO DEL SERVIZIO DI AFFIANCAMENTO AL RPD PER L'ATTUAZIONE DI UN PROGRAMMA DI AUDIT PRIVACY DI PRIMA PARTE PER ACI E LA SUA FEDERAZIONE, DA AGGIUDICARE CON IL CRITERIO DELL'OFFERTA ECONOMICAMENTE PIÙ VANTAGGIOSA SULLA BASE DEL MIGLIOR RAPPORTO QUALITÀ/PREZZO

CIG: A00EFFBA94

CUI: S00493410583202300007

CPV: 79212200-5

Automobile Club d'Italia

Sommario

1 INTRODUZIONE

L'Automobile Club d'Italia (ACI) è un Ente pubblico non economico senza scopo di lucro a base associativa, che tutela e rappresenta gli interessi dell'automobilismo italiano, del quale promuove lo sviluppo attraverso la diffusione della cultura della mobilità. L'ACI svolge servizi istituzionali e delegati dallo Stato, attraverso le sedi periferiche e gli Automobile Club territoriali federati (AC), avvalendosi anche delle proprie Società strumentali.

L'ACI, inoltre, è la Federazione che associa 98 Automobile Club sul territorio (AC), i quali, anch'essi, come l'ente Federante, sono enti Pubblici non economici autonomi a base associativa e perseguono le stesse finalità dell'ACI, svolgendo ogni attività utile alla valorizzazione e al sostegno dei Soci e dell'automotive in generale.

L'insieme dei Sodalizi rappresenta una compagine ampia e ramificata, operativa in ambito nazionale, alla quale sono attribuiti compiti di raccordo gestionale con le funzioni direttive dell'ACI, di cui recepiscono obiettivi, piani e programmi, nonché di rappresentanza istituzionale e di presidio del territorio, anche in termini di fattiva collaborazione e sinergia nel presidio delle attività elencate all'art. 2 dello Statuto dell'Ente, complessivamente volte al conseguimento degli scopi ad esso attribuiti, tra i quali si annoverano la promozione dell'associazionismo e dello sport automobilistico.

Gli Automobile Club territoriali sono a loro volta dotati di un proprio network di "Punti ACI", tradizionalmente definiti Delegazioni ACI, distribuiti sul territorio nazionale in modo capillare, per una concorrenza di oltre 1500 "PdV" aperti su strada e ad intensa pedonabilità, i quali, come anche indicato all'art. 5 lett. c) dello Statuto dell'ACI, contribuiscono al rafforzamento del ruolo dell'Ente nell'erogazione dei servizi che sono o potranno essere a questo delegati o affidati dallo Stato, dalle Regioni o da altri Enti pubblici.

In linea con le previsioni dettate dalla normativa euro comunitaria in materia di tutela dei dati personali, Reg. (UE) n.679/2016 (GDPR), art. 37 comma 1 lett. a), l'ACI ha nominato un Responsabile per la protezione dei dati personali (RPD); analogamente, ogni AC territoriale, federato all'Automobile Club d'Italia ai sensi dell'art. 1 dello Statuto dell'Ente e come stabilito nel Regolamento interno della Federazione ACI ha nominato un proprio Responsabile della protezione dei dati (RPD) coincidente con il RPD dell'ACI in un'ottica di omogeneità organizzativa interna del sistema di data governance della Federazione ACI.

Tenuto conto dell'articolazione della Federazione ACI e considerato il vigente quadro regolamentare europeo e nazionale in materia di protezione dei dati personali, l'obbligo di sorveglianza posto in capo al RPD è esteso anche ai 98 Automobile Club presenti sul territorio nazionale, i quali svolgono attività che possono prevedere il trattamento di dati personali di particolare complessità e rilevanza.

2 OGGETTO DELLA FORNITURA

L'attività oggetto della fornitura si inquadra nell'ambito dei compiti assegnati al Responsabile della protezione dei dati personali (RPD), dagli artt. 38 e 39 del GDPR, dalle Linee guida sui responsabili della protezione dei dati – WP243, adottate dal Gruppo di lavoro art. 29 il 13 dicembre 2016,

nonché dal Manuale RPD, sviluppato per il programma "T4DATA", nella versione approvata dalla Commissione nel luglio 2019, ed infine dal "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico", adottato dal Garante per la protezione dei dati con provvedimento n. 196 del 29 aprile 2021 ai sensi dell'art. 57, par. 1, lett. b) e d), del GDPR e dell'art. 154-bis, comma 1, lett. a) del decreto legislativo n. 196/2013 e s.m.i. - Codice Privacy.

La fornitura consiste nella realizzazione di un'attività di audit privacy di prima parte per la verifica della conformità del modello di data governance impiegato dalle Strutture dell'Ente e dalla Federazione ACI alla disciplina in materia di tutela dei dati personali, anche al fine di migliorarne la gestione attraverso azioni preventive/correttive e strumenti, specificamente individuati, di monitoraggio e verifica; ciò al fine di garantire l'osservanza dei principi e delle regole della protezione dati, che costituiscono un necessario presupposto per assicurare la tutela dei diritti e delle libertà fondamentali delle persone fisiche.

All'Operatore economico sono richieste le seguenti attività:

1. Nella **fase di studio e analisi** preliminare dei Modelli esistenti:
   - **a.** fare proprio e ottimizzare - anche con l'ausilio di strumenti di Office automation - il "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali" attualmente adottato dal RPD dell'ACI e della Federazione;
   - **b.** predisporre il piano dettagliato degli audit da svolgere, comprensivo delle fasi necessarie - analisi del contesto organizzativo e dei processi, preparazione degli audit, attività sul campo, fasi di consuntivazione, follow-up e verifica dell'efficacia delle azioni correttive e di miglioramento definite sulla base dei risultati - per raggiungere gli obiettivi stabiliti e condivisi con il RPD;

2. Nella **fase esecutiva**:
   - **a.** coadiuvare il RPD nella verifica del grado di adempimento alla normativa europea e nazionale in materia di protezione dei dati personali da parte di:
     - n. 42 Funzioni ed Uffici Centrali dell'ACI (Sede centrale di Roma);
     - n. 3 Aree professionali (Legale, Tecnica, Statistica).
     - n. 98 AC, Enti territoriali autonomi federati all'ACI;

     La suddetta articolazione delle strutture potrebbe variare in caso di modifica degli assetti organizzativi della Federazione.
     Prevedendo come *modalità di esecuzione*:
     - Audit alle Funzioni/ Uffici/Aree professionali Centrali: tutte in presenza, sede di Roma;
     - Audit agli AC: n. 3/anno in presenza presso la sede dell'AC;
     - Audit ai restanti 89 AC, in modalità videoconferenza.

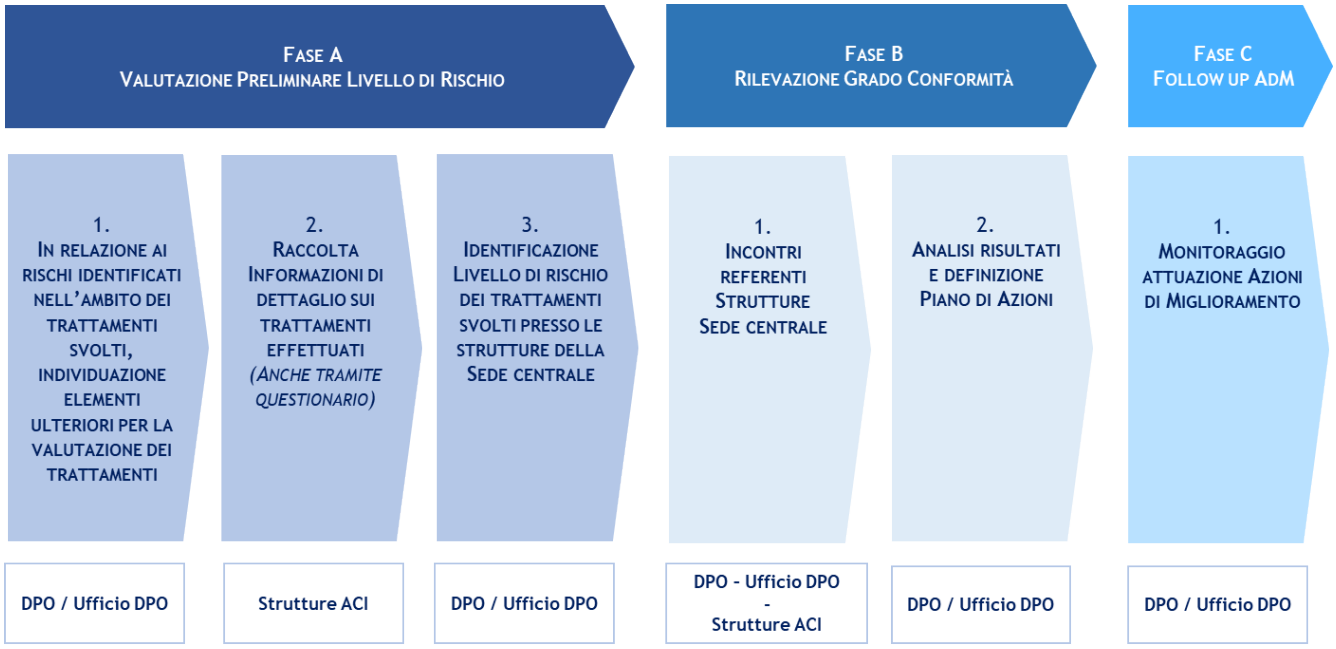
     Luogo di esecuzione:
     - Roma, via Marsala, presso la Sede Centrale dell'Ente per le 45 Funzioni ed Uffici Centrali e Aree Professionali Tecniche
     - indicativamente, presso le sedi degli Automobile Club territoriali di Milano, Roma, Torino, Salerno, Bologna, Firenze, Bari, Genova, Modena, salvo

diverse esigenze che dovessero manifestarsi in corso d'opera.

b. Fornire supporto al RPD nell'implementazione della metodologia attualmente adottata per le verifiche di cui sopra anche con l'ausilio di strumenti di Office automation.

c. Conservare in apposita repository e mettere a disposizione del RPD la documentazione di supporto utilizzata per lo svolgimento dell'attività di audit.

Per una migliore rappresentazione delle attività richieste, si riporta, di seguito, il framework del Sistema di valutazione adottato.



3 SPECIFICHE DELLA FORNITURA E ITER PROCEDURALE

L'Aggiudicatario dovrà svolgere le attività richieste secondo la prassi professionale prevista in ambito di internal auditing, adottando un comportamento orientato all'ascolto attivo, anche con l'applicazione delle tecniche di audit descritte nella ISO 19011:2018 al fine di favorire un processo di comunicazione efficace finalizzato alla massimizzazione del senso di responsabilità degli attori coinvolti (Strutture dell'ACI e della Federazione ACI).

Nel triennio di vigenza contrattuale, l'iter procedurale delle fasi di cui al precedente paragrafo 2 del presente Capitolato, dovrà necessariamente articolarsi come segue:

1. <u>Fase di studio e analisi preliminare dei Modelli relativi al "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali":</u>

   - lo studio del contesto della Federazione ACI e dei processi rilevanti relativi alle attività svolte;
   - un'analisi degli attuali Modelli di gestione dei dati predisposti secondo la metodologia di valutazione del grado di conformità agli aspetti in materia di protezione dei dati

personali anche ai fini di ottimizzarli e adattarli alle varie tipologie di Strutture della Federazione;

- l'elaborazione su base semestrale, per l'intera durata contrattuale, di un resoconto degli esiti dell'attività di audit realizzata ivi compresa quella di ottimizzazione del Modello;
- l'aggiornamento tempestivo, per l'intera durata contrattuale, del Modello ogniqualvolta siano apportate variazioni normative che impattano sul sistema di gestione dei dati personali e/o intervengano variazioni agli assetti organizzativi della Federazione;
- l'effettuazione, nel caso di aggiornamenti del modello, di appositi incontri con il *Management* dell'ACI e degli AACC;

2. <u>Fase di esecuzione: supporto al RPD nella verifica del grado di adempimento alla normativa in materia di protezione dei dati personali:</u>

   A. preparazione degli audit, con incontri con il RPD e attraverso l'acquisizione e l'esame della documentazione esistente relativa all'oggetto della fornitura;
   B. predisposizione di un piano dettagliato degli audit da svolgere nel triennio, con l'indicazione del timing di:
      a. audit in presenza e da remoto tramite videoconferenza;
      b. consuntivazione/reportistica specifica;
      c. follow-up;
   C. elaborazione e consegna al RPD di un audit report e di un remediation plan per ciascuna Struttura ACI/AC intervistata;
   D. elaborazione documentazione di follow-up e di verifica dell'efficacia delle azioni correttive e di miglioramento definite sulla base dei risultati per raggiungere gli obiettivi stabiliti e condivisi con il RPD.

Le prestazioni oggetto del servizio dovranno essere svolte da un gruppo di lavoro costituito come meglio specificato al paragrafo 4 e proposto in offerta tecnica dal concorrente aggiudicatario e, comunque, nel rispetto di quanto previsto dal presente Capitolato.

In particolare, le prestazioni definite al paragrafo precedente ai punti 1 e 2, dovranno essere erogate dal gruppo di lavoro e consistere, a titolo esemplificativo e non esaustivo, nelle seguenti attività:

A. **indagine preliminare** finalizzata ad approfondire la conoscenza delle principali caratteristiche delle attività/processi che dovranno costituire oggetto dell'audit con individuazione/valutazione del livello di rischio (o grado di funzionamento del sistema);
B. **pianificazione delle attività (Piano di Audit)** ovvero definizione degli specifici interventi previsti in relazione ai servizi richiesti dal management con indicazione dei tempi di avvio e di conclusione per ogni intervento e degli oggetti dell'audit (processi o rischi);
C. **esecuzione dell'incarico** ossia concreto svolgimento di ciascun intervento incluso nel Piano di Audit al quale dovrà conseguire la definizione di tutte le operazioni compiute dall'Operatore economico per raccogliere la documentazione necessaria (audit evidence) a supportare le proprie conclusioni.
D. **rapporto di audit** ovvero il documento che chiude formalmente l'intervento di audit. Con tale

rapporto l'Operatore economico segnala al RPD dell'Ente e ai destinatari dello stesso le principali criticità emerse dal lavoro e le raccomandazioni circa l'esecuzione di azioni che consentano di apportare idonei miglioramenti ai processi indagati;

E. **follow up** ovvero la sequenza di azioni tramite le quali gli auditor si accertano dell'efficacia e tempestività delle azioni correttive intraprese in risposta ai rilievi da loro comunicati alle Strutture

Tutte le fasi sopra indicate saranno eseguite dal gruppo di lavoro con il supporto e la collaborazione del RPD dell'ACI e dai funzionari da lui individuati e con la partecipazione del *Management* di ACI e degli AACC.

4 TEAM DI LAVORO

Le risorse da impiegare nell'affidamento dovranno rispondere ai requisiti previsti dai profili di seguito descritti, laddove i requisiti espressi sono considerati requisiti minimi.
In particolare, l'espletamento delle attività in precedenza descritte avverrà a mezzo di apposito gruppo di lavoro composto da n. 4 risorse rispondenti ai profili di seguito descritti:

1) ***n. 1 professionista senior*** in possesso di:
   - diploma di laurea magistrale ovvero specialistica ovvero conseguita ai sensi del vecchio ordinamento che includa almeno una materia afferente alle tematiche relative alla protezione di persone, luoghi, dati sensibili e rete, compliance, cyber e risk management;
   - esperienza lavorativa di almeno tre anni maturata nel quinquennio antecedente la data di pubblicazione della presente procedura nella costruzione e gestione di sistemi di tutela della protezione dati personali e del diritto informativo per lo svolgimento delle attività correlate e conseguenti, svolta presso pubbliche amministrazioni ed avente ad oggetto la materia dei dati personali e della loro libera circolazione come disciplinato dal Regolamento EU 679/2016 e dal D.lgs. 196/2003.

   Al Professionista Senior viene richiesto di garantire ed assicurare:
   la coerenza e l'allineamento di tutti i servizi in esecuzione costituendo l'interfaccia operativa principale nei confronti del RPD; la corretta esecuzione dell'affidamento attenendosi alle disposizioni contrattuali e il pieno rispetto dei livelli di servizio; il coordinamento dell'intero gruppo di lavoro, assicurando piena coerenza con le linee strategiche e gli obiettivi definiti; la disponibilità delle risorse, garantendo la flessibilità del gruppo di lavoro; il monitoraggio delle iniziative in corso, garantendo l'efficacia, l'efficienza e la tempestività delle attività, facendosi portatore delle problematiche rilevate nell'esecuzione delle attività, proponendo soluzioni e intraprendendo le necessarie azioni correttive; il rispetto delle tempistiche oggetto del contratto.

2) ***n. 2 professionisti specialist*** in possesso di:
   - diploma di laurea magistrale ovvero specialistica ovvero conseguita ai sensi del vecchio ordinamento che includa almeno una materia afferente alle tematiche relative alla protezione di persone, luoghi, dati sensibili e rete, compliance, cyber e risk

management;
- esperienza lavorativa di almeno tre anni nel profilo di professionista specialist in gruppi di lavoro che hanno operato nella costruzione e gestione di sistemi di tutela della protezione dati personali e del diritto informativo per lo svolgimento delle attività correlate e conseguenti, presso committenti pubblici o privati.

Il Professionista Specialist garantisce:
la corretta esecuzione dei servizi a lui assegnati curandone gli aspetti sia tecnici sia gestionali, risolve in autonomia le problematiche di processo e organizzative rilevate durante l'esecuzione delle azioni affidate, allineandosi costantemente con il committente; partecipa attivamente al lavoro di team e cura la produzione dei documenti richiesti, nei tempi stabiliti.

3) ***n. 1 professionista specialist in ambito informatico*** in possesso di:
- diploma di laurea magistrale ovvero specialistica ovvero conseguita ai sensi del vecchio ordinamento in ingegneria informatica o elettronica oppure in scienze e tecnologie informatiche o altro corso di laurea equivalente;
- esperienza lavorativa di almeno tre anni nell'attività di progettazione, realizzazione e gestione dei software, dei sistemi, dei dispositivi e delle infrastrutture ed elaborazione dei dati e delle informazioni con particolare riguardo alla gestione delle tematiche inerenti l'ingegneria della privacy e cybersecurity, data breach, gestione dei dati personali ad esse collegati, presso committenti pubblici o privati.

Il Team deve prevedere nella sua composizione il rispetto di una quota di occupazione giovanile, under 36, e/o femminile corrispondente ad almeno una risorsa

L'Operatore economico dovrà garantire, con continuità per tutta la durata dell'affidamento, un qualificato supporto tecnico ed operativo alla struttura committente nella realizzazione di tutte le attività oggetto dell'appalto, in conformità a quanto indicato nel presente paragrafo ed all'offerta tecnica presentata in sede di partecipazione alla gara, secondo quanto indicato nei paragrafi 18.1 e seguenti del disciplinare di gara.

È prevista, per l'Amministrazione contraente, la possibilità di richiedere sostituzioni/integrazioni di risorse con specifiche competenze, non esplicitamente riportate nei profili sopra descritti.
Nell'arco dell'intera durata dell'affidamento, i relativi profili professionali saranno considerati invariati, anche in caso di aumento di qualifica, nel caso la loro fruizione si riferisca alla medesima attività o ad attività di pari livello.

5 TEMPI E DURATA DELL'INCARICO

L'incarico avrà durata triennale a partire dalla data di sottoscrizione del contratto.

Di seguito si riportano, i risultati attesi previsti per ciascuna annualità rispetto a quanto indicato nel dettaglio ai paragrafi 2 e 3:

- **Prima annualità:**

1) documento attestante l'avvenuto studio/analisi del "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali" (entro 2 mesi dalla data di sottoscrizione del contratto);
2) piano dettagliato degli audit da svolgere nel triennio prevedendo, per ciascuna struttura, l'attività di follow up entro il termine della stessa annualità di svolgimento (entro 2 mesi dalla data di sottoscrizione del contratto);
3) effettuazione, secondo la calendarizzazione proposta, degli audit con il management dell'ACI e degli AC a n. 32 AC e n. 15 Funzioni ed Uffici Centrali;
4) redazione dei relativi audit report e remediation plan;
5) elaborazione delle relazioni sullo stato avanzamento lavori: una al I semestre e la seconda per l'intera annualità di riferimento;
6) documentazione di follow up delle strutture oggetto di audit con verifica dell'efficacia delle azioni correttive e di miglioramento definite
7) proposte di ottimizzazione del "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali"

- **Seconda annualità:**

1) effettuazione, secondo la calendarizzazione proposta, degli audit con il management dell'ACI e degli AC a n. 33 AC e n. 15 Funzioni ed Uffici Centrali;
2) redazione dei relativi audit report e remediation plan;
3) elaborazione delle relazioni sullo stato avanzamento lavori: una al I semestre e la seconda per l'intera annualità;
4) documentazione di follow up delle strutture oggetto di audit con verifica dell'efficacia delle azioni correttive e di miglioramento definite
5) proposte di ottimizzazione del "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali"

- **Terza annualità:**

1) effettuazione, secondo la calendarizzazione proposta, degli audit con il management dell'ACI e degli AC a n. n. 33 AC + n.12 Funzioni e Uffici Centrali e n. 3 Aree Professionali.
2) redazione dei relativi audit report e remediation plan;
3) redazione delle relazioni sullo stato avanzamento lavori: una al I semestre e la seconda per l'intera annualità ;
4) documentazione di follow up delle strutture oggetto di audit con verifica dell'efficacia delle azioni correttive e di miglioramento definite
5) proposte di ottimizzazione del "Sistema per la valutazione di conformità delle strutture dell'ACI e degli AC agli aspetti in materia di Protezione Dati Personali"