CLUB ALPINO ITALIANO

Sede Centrale

Via E. Petrella 19 – 20124 Milano

Tel. 02.205723.1 – Fax 02.205723.201

www.cai.it

Affidamento ai sensi dell'art. 50 comma 1 lettera b) del D. Lgs. n. 36/2023 del Servizio di Data Protection Officer (DPO) e di supporto alla corretta applicazione del Regolamento Europeo sulla protezione dei dati personali (GDPR) 2016/679

Scheda Tecnica

PREMESSA

Il Club Alpino Italiano è una libera associazione nazionale che, come recita l'articolo 1 del suo Statuto, «*ha per scopo l'alpinismo in ogni sua manifestazione, la conoscenza e lo studio delle montagne, specialmente di quelle italiane, e la difesa del loro ambiente naturale*». Il CAI si configura come un ente pubblico non economico, mentre tutte le sue strutture territoriali (Sezioni, Gruppi Regionali e Provinciali) sono soggetti di diritto privato. L'Associazione è costituita da Soci e Socie (367.848 al 31 dicembre 2025), che partecipano alle attività di 524 Sezioni e 308 Sottosezioni appartenenti a 19 Gruppi Regionali, 2 Raggruppamenti Provinciali (Trentino e Alto Adige) e tre Sezioni Nazionali.

Il Club Alpino Italiano (CAI), ente pubblico non economico a base associativa con sede legale in Milano, è tenuto alla designazione obbligatoria del Responsabile della protezione dei dati – RPD/DPO, ai sensi dell'articolo 37, paragrafo 1, lettera a) del Regolamento generale sulla protezione dei dati (RGPD/GDPR) - Regolamento (UE) 2016/679. Lo stesso articolo 37 del predetto Regolamento al paragrafo 6, inoltre, prevede che il Responsabile della protezione dei dati può "*assolvere i suoi compiti in base a un contratto di servizi*".
In considerazione delle citate premesse il CAI intende procedere all'affidamento del servizio di *Data Protection Officer (DPO)* e di supporto alla corretta applicazione del GDPR, per la durata di 24 mesi.

ART. 1 – OGGETTO DEL CONTRATTO

La presente Scheda tecnica disciplina le prestazioni di contratto avente ad oggetto il servizio di "Responsabile della protezione dei dati" ("*Data Protection Officer*" di seguito DPO) e di supporto specialistico alla corretta applicazione del Regolamento Europeo sulla protezione dei dati personali 2016/679.
L'incarico di DPO sarà svolto in piena autonomia ed indipendenza e comporterà l'espletamento delle prestazioni di cui all'art. 39 del GDPR, riportate di seguito:

- 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 GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del predetto 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;
- fornire, se richiesto, un parere in merito alla eventuale DPIA e sorvegliarne lo svolgimento ex art. 35 del GDPR;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ex art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il DPO dovrà fornire anche le seguenti ulteriori attività riportate in via generale e a titolo esemplificativo, finalizzate ad assicurare la corretta applicazione del GDPR:

a) verificare l'esattezza e la completezza dei trattamenti inseriti nel Registro dei trattamenti, provvedendo ai necessari aggiornamenti, alla tenuta dello stesso e alla consultabilità da parte delle componenti dell'ente;
b) fornire consulenza in merito agli obblighi vigenti relativi alla protezione dei dati;
c) rispondere a singoli quesiti istituzionali in materia di privacy entro 5 giorni lavorativi dall'inoltro;
d) fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e

all'esercizio dei relativi diritti;

e) programmare e curare l'attività di sensibilizzazione e formazione del personale CAI che partecipa ai trattamenti e alle connesse attività di controllo per almeno una sessione l'anno; ad ogni partecipante dovrà essere rilasciata certificazione idonea a comprovare la partecipazione;
f) fornire supporto nella definizione, sulla base dei rischi emersi in fase di valutazione, delle priorità delle attività da svolgere;
g) riportare alla direzione dell'amministrazione quanto pertinente alla funzione, fornendo una relazione annuale sulle attività svolte e sul livello di conformità al GDPR;
h) fornire assistenza in merito al rispetto di adeguati livelli interni di conformità al GDPR;
i) predisporre ed eseguire almeno un audit interno all'anno; le attività di audit devono risultare da apposito verbale nel quale saranno evidenziate eventuali non conformità riscontrate e le prescrizioni o raccomandazioni necessarie od opportune;
j) dare supporto nella gestione della documentazione attestante in maniera oggettiva e trasparente le attività effettuate per garantire la conformità al GDPR, fungendo da punto di contatto per l'esibizione a terzi;
k) garantire piena disponibilità a partecipare a questioni inerenti la protezione dei dati;
l) fornire parere in ordine alla legittimità ed alla correttezza di nuovi Trattamenti dei dati personali eventualmente emergenti;
m) coadiuvare il CAI nella predisposizione e nell'adeguamento di linee guida, modello organizzativo, indicazioni operative, modulistica, flussi di lavoro, informative e policy applicative in materia di trattamento e protezione dei dati personali (anche in coordinamento con gli ambiti di sicurezza informatica), nonché per ogni atto o adempimento in relazione al quale il CAI ritiene di dover acquisire un parere preventivo;
n) organizzare riunioni periodiche con i referenti interni coinvolti nell'attuazione delle misure di sicurezza al fine di fornire un allineamento sull'evoluzione normativa e sulle conseguenti implicazioni sul sistema di gestione privacy;
o) valutare gli impatti di nuove progettualità sulla protezione dei dati personali (*privacy by design e by default*);
p) supportare le articolazioni dell'ente nella valutazione delle richieste di accesso agli atti che comportino riflessi sulla protezione dei dati personali, nell'ottica di contemperare il diritto di accesso e il diritto di riservatezza dei dati trattati;
q) fornire supporto per la predisposizione e l'aggiornamento del registro degli eventi avversi, nonché per l'istruttoria degli stessi, attraverso riscontri per iscritto, entro tempistiche compatibili con i termini di notifica di violazione al Garante per la protezione dei dati personali;
r) collaborare e coordinarsi con i DPO eventualmente designati dai responsabili del trattamento che trattino dati per conto del CAI o con i DPO nominati dai Titolari per i quali il CAI svolge il ruolo di Responsabile del trattamento;
s) individuare situazioni di contitolarità del trattamento e, in tali ipotesi, predisporre e mettere a disposizione i relativi accordi di contitolarità.

Il DPO si rapporterà con con le articolazioni dell'ente coinvolte e la Direzione, qualora quest'ultima lo richieda, e dovrà assicurare:

- la presenza fisica presso la sede del CAI tutte le volte che lo si reputi necessario o la connessione audio/video da remoto, se ritenuta sufficiente dai referenti CAI;
- la presenza fisica in caso di visite ispettive dell'Autorità di controllo, entro un termine massimo di 24 ore dalla richiesta formulata da parte del CAI e per tutta la durata delle attività;
- il riscontro – per iscritto e con pareri adeguatamente argomentati – per un numero illimitato di richieste formulate dal CAI in ordine a tutte le questioni concernenti l'oggetto dell'incarico, entro 5 (cinque) giorni lavorativi o nel termine più breve indicato dall'affidatario;
- la reperibilità telefonica o tramite e-mail nei giorni lavorativi e durante il normale orario di lavoro osservato dal personale del CAI.

Il DPO, inoltre, dovrà garantire di poter essere contattato in modo semplice e diretto, oltre che dai dipendenti del CAI, dall'Autorità di controllo e dagli interessati. A tal fine dovrà mettere a disposizione mezzi idonei e sicuri di comunicazione che consentano un contatto tempestivo e in ogni caso dovrà fornire almeno un contatto telefonico e una casella di posta elettronica dedicati.

I dati di contatto ed il nominativo del DPO saranno pubblicati sul sito aziendale istituzionale e comunicati alle competenti autorità di controllo.
Tutte le risorse strumentali necessarie per lo svolgimento del servizio, quali attrezzature tecniche o informatiche, mezzi di trasporto, linee telefoniche, sono a completo ed esclusivo carico dell'affidatario.
Al DPO sarà consentito l'accesso agli uffici CAI al fine di acquisire notizie, informazioni e documenti necessari per lo svolgimento dei propri compiti. L'accesso sarà preceduto, di norma, da apposita comunicazione ai responsabili delle strutture interessate.
Il DPO, anche successivamente alla cessazione del rapporto contrattuale, in relazione ai dati e informazioni di cui venga a conoscenza in occasione dell'adempimento dell'incarico, ha l'obbligo di:

- garantire la segretezza impegnandosi ad impedire qualsiasi divulgazione;
- non eseguire copie, estratti, note od elaborazioni di qualsiasi genere e non permettere che altri ne eseguano;
- non farne oggetto di utilizzazione per scopi diversi da quelli strettamente necessari all'esecuzione dello stesso.

ART. 2 – ATTIVITÀ PRELIMINARI

In via preliminare, il DPO deve effettuare un'analisi dell'assetto complessivo del CAI e la verifica della completezza e conformità agli adempimenti in materia di trattamento e sicurezza dei dati, fornendo entro 60 giorni dall'affidamento del servizio, una relazione che evidenzi il relativo grado di conformità, le azioni da intraprendere e il conseguente piano di lavoro.
Nella redazione del piano di lavoro, il DPO dovrà proporre, tra l'altro, in accordo con il CAI le azioni formative finalizzate a promuovere la cultura della protezione dei dati.
Effettuate le verifiche e le ricognizioni anzidette, l'affidatario dovrà, in via prioritaria, implementare l'impianto esistente con riguardo, in particolare:

- alla predisposizione/aggiornamento/implementazione, in collaborazione con il CAI, del modello organizzativo privacy finalizzato alla distribuzione delle responsabilità interne in ordine al trattamento dei dati, e della regolamentazione e linee guida aziendali in tema di trattamento dei dati personali;
- alla predisposizione/aggiornamento/implementazione, in collaborazione con il CAI, di una procedura di gestione degli incidenti di sicurezza/data breach e alla conseguente predisposizione/tenuta/aggiornamento periodico, ovvero quando richiesto, del Registro di violazione dei dati;
- alla predisposizione e periodico riesame/aggiornamento, anche mediante gestionali informatizzati messi a disposizione dallo stesso affidatario, delle eventuali "valutazioni di impatto" (Data Protection Impact Assessment DPIA) in particolare quelle considerate obbligatorie dalla normativa e comunque secondo un ordine di priorità definito in accordo con il CAI e alla individuazione delle idonee misure organizzative e tecniche atte a garantire le prescrizioni normative, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

ART. 3 – REQUISITI DELL'INCARICO

In base all'articolo 38, paragrafo 6, del GDPR al Responsabile della protezione dei dati è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "*tali compiti e funzioni non diano adito a un conflitto di interessi*".
In caso di affidamento ad un soggetto giuridico, il ruolo di DPO dovrà essere assunto dal legale rappresentante del soggetto offerente o da persona da esso espressamente delegata, che ne risponderà a tutti gli effetti di legge.
Il DPO dovrà operare in assenza di conflitto di interessi, in modo autonomo ed indipendente, interfacciandosi con il personale del CAI e, nell'eseguire i propri compiti, dovrà tenere in debita considerazione i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
All'atto dell'affidamento, il DPO e le eventuali figure di supporto di cui si avvale dovranno rendere

apposita dichiarazione di insussistenza di conflitti di interesse.
L' affidatario è responsabile dell'osservanza da parte dei propri dipendenti delle disposizioni di ordine interno che dovessero essere emanate dal CAI, che potrà richiedere, in qualsiasi momento, dandone adeguata motivazione.
L' affidatario è tenuto a sostituire il personale messo a disposizione qualora non sia ritenuto idoneo dal CAI, su segnalazione motivata del Direttore dell'Esecuzione del Contratto, senza che l'affidatario possa sollevare eccezioni alla richiesta ricevuta.
Il CAI, in qualsiasi momento dell'esecuzione del contratto, ha la facoltà di esprimere, attraverso il Direttore dell'Esecuzione del Contratto, il giudizio in ordine alla idoneità tecnico-qualitativa delle prestazioni erogate dal personale designato dall'affidatario e eventualmente richiederne, nel caso di giudizio negativo, la sostituzione entro un termine di 10 giorni dalla richiesta.
La mancata sostituzione entro il termine assegnato, ovvero la reiterata assegnazione di personale privo dei requisiti richiesti, costituisce grave inadempimento contrattuale e comporta l'applicazione delle penali previste dal presente Capitolato, fatto salvo il diritto del CAI di procedere alla risoluzione del contratto nei casi e con le modalità previste dalla normativa vigente e dal contratto.

ART. 4 – LIVELLI DI SERVIZIO

L'Affidatario è tenuto a garantire, per tutta la durata del contratto, i livelli minimi di servizio di seguito riportati.

Prestazione	Livello di servizio richiesto
Riscontro ai quesiti formulati dal CAI	Entro 5 giorni lavorativi dal ricevimento della richiesta o, per quelli urgenti, entro il termine più breve e consono all'evasione
Supporto in caso di violazione dei dati personali (data breach)	Rigorosamente nei tempi utili a garantire il rispetto dei termini previsti dal GDPR
Partecipazione a riunioni convocate dal CAI	Riscontro entro 3 giorni lavorativi, salvo urgenze
Presenza in occasione di ispezioni dell'Autorità Garante o di altre Autorità competenti	Entro 24 ore dalla richiesta del CAI, ovvero immediatamente da remoto qualora ritenuto sufficiente
Disponibilità telefonica ed e-mail	Nei giorni lavorativi, dalle ore 8:30 alle ore 17:30
Supporto aggiornamento del Registro dei trattamenti e della documentazione privacy	Entro 30 giorni dall'avvio del trattamento
Redazione e aggiornamento delle DPIA richieste	Entro 15 giorni dalla richiesta, salvo casi di particolare complessità concordati con il CAI
Relazione annuale sullo stato di conformità	Entro il 31 gennaio dell'anno successivo o diverso termine concordato con il CAI
Attività di Audit	Almeno un audit annuale, secondo il Piano delle attività concordato
Attività formative	Almeno una sessione formativa annuale, con rilascio dell'attestato ai partecipanti

L'Affidatario dovrà monitorare il rispetto dei livelli di servizio e darne evidenza nelle comunicazioni periodiche, segnalando per ciascun indicatore il livello previsto, il livello effettivamente conseguito, le eventuali criticità riscontrate e le azioni correttive adottate.

Il mancato rispetto dei livelli di servizio costituisce inadempimento contrattuale e comporta l'applicazione delle penali previste dal presente Capitolato, fatto salvo il risarcimento dell'eventuale maggior danno.

ART. 5 – ASSICURAZIONI E RESPONSABILITÀ

L'affidatario dovrà obbligatoriamente stipulare e mantenere attiva per tutta la durata dell'incarico una polizza assicurativa di Responsabilità Civile Professionale che tenga indenne la Stazione Appaltante da tutti i rischi connessi all'esecuzione dell'appalto da qualsiasi causa determinata.

La polizza dovrà prevedere la copertura dei danni causati da perdita, distruzione, furto o diffusione non autorizzata di dati personali ivi comprese le sanzioni derivanti dal mancato o errato adempimento alle prescrizioni normative derivanti dal Regolamento UE in materia di protezione dati personali.

Il massimale della polizza assicurativa è stabilito, come importo minimo, in € 1.000.000,00 per sinistro/anno o in misura corrispondente alla sanzione massima prevista dall'art. 83 Regolamento UE. In alternativa alla stipulazione della polizza che precede, l'affidatario potrà dimostrare l'esistenza di una polizza assicurativa, già attivata, avente le medesime caratteristiche indicate per quella specifica. In tal caso, l'affidatario dovrà produrre un'appendice alla stessa, nella quale si espliciti chela polizza in questione copre anche i servizi previsti dal contratto in argomento, fermo restando, in ogni caso, l'obbligo di manleva assunto dall'affidatario.

ART. 6 – PENALI

Fatte salve le ulteriori responsabilità previste dalla normativa vigente e il risarcimento dell'eventuale maggior danno, il CAI, previa contestazione scritta dell'inadempimento e valutate le eventuali controdeduzioni dell'Affidatario, potrà applicare le seguenti penali:

Inadempimento	Penale
Ritardo nella risposta ai quesiti rispetto ai termini contrattualmente previsti	€ 100,00 per ogni giorno lavorativo di ritardo
Ritardo nella consegna della relazione annuale	€ 300,00 per ogni giorno di ritardo
Mancata effettuazione della sessione formativa annuale entro i termini concordati	€ 1.000,00 per ogni evento
Mancata esecuzione dell'audit annuale	€ 1.500,00 per ogni audit non eseguito
Mancata presenza, senza giustificato motivo, in occasione di ispezioni dell'Autorità Garante o di altri organismi competenti	€ 3.000,00 per ogni evento
Mancato rispetto dei tempi di presa in carico di un evento di data breach previsti dal contratto	€ 2.000,00 per ogni evento
Mancata partecipazione senza giustificato motivo a riunioni convocate dal CAI	€ 500,00 per ogni evento
Mancata consegna della documentazione finale e delle attività di handover alla scadenza del contratto	€ 2.000,00
Mancata sostituzione del personale giudicato inidoneo dal CAI entro il termine di 10 giorni lavorativi	€ 500,00 per ogni giorno di ritardo oltre il termine assegnato, fino ad un massimo del 10% del valore contrattuale relativo alla prestazione

L'applicazione delle penali non esclude l'obbligo dell'Affidatario di eseguire comunque le prestazioni dovute.

Le penali saranno applicate previa contestazione scritta dell'inadempimento. L'Affidatario potrà presentare le proprie controdeduzioni entro cinque giorni lavorativi dal ricevimento della contestazione. IL CAI valuterà le eventuali giustificazioni e, qualora non le ritenga fondate, procederà all'applicazione della penale mediante compensazione con i corrispettivi maturati o mediante escussione della garanzia definitiva, ove prestata.
L'importo complessivo delle penali applicate non potrà superare il dieci per cento (10%) dell'importo contrattuale complessivo, fatto salvo il diritto del CAI alla risoluzione del contratto nei casi di grave o reiterato inadempimento e al risarcimento dell'eventuale maggior danno.
Costituiscono, in particolare, grave inadempimento:

- il mancato svolgimento di due audit annuali consecutivi;
- la reiterata violazione dei livelli di servizio (SLA) per almeno cinque episodi nell'arco di dodici mesi;
- l'assenza ingiustificata in occasione di ispezioni disposte dall'Autorità Garante;
- il mancato mantenimento dei requisiti professionali richiesti per l'incarico;
- la sussistenza di situazioni di conflitto di interessi non tempestivamente comunicate.

ART. 7 – OBBLIGHI DELL'ENTE

Il CAI si obbliga, nel corso dell'affidamento a:

- mettere a disposizione del RPD individuato le risorse adeguate al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
- non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
- garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.